Configuración y administración de vSphere with Tanzu

Actualización 3
VMware vSphere 7.0
vCenter Server 7.0
VMware ESXi 7.0



Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

https://docs.vmware.com/es/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Contenido

Configuración y administración de vSphere with Tanzu 12

1 Información actualizada 13

2 Conceptos de vSphere with Tanzu 18

¿Qué es vSphere with Tanzu? 18

¿Qué es un pod de vSphere? 21

¿Qué es un clúster de Tanzu Kubernetes? 23

Cuándo utilizar pods de vSphere y clústeres de Tanzu Kubernetes 26

Usar máquinas virtuales en vSphere with Tanzu 26

Flujos de trabajo y funciones de usuario de vSphere with Tanzu 28

¿Cómo cambia vSphere with Tanzu el entorno de vSphere? 40

Licencias para vSphere with Tanzu 41

3 Arquitectura y componentes del vSphere with Tanzu 44

Arquitectura de vSphere with Tanzu 44

Arquitectura del servicio Tanzu Kubernetes Grid 48

Modelo de tenant del clúster de Tanzu Kubernetes 50

Autenticación de vSphere with Tanzu 51

Redes de vSphere with Tanzu 53

Seguridad de vSphere with Tanzu 53

Almacenamiento de vSphere with Tanzu 54

4 Redes para vSphere with Tanzu 58

Redes del clúster supervisor 58

Redes de clústeres de servicio Tanzu Kubernetes Grid 64

Configurar NSX-T Data Center para vSphere with Tanzu 65

Requisitos del sistema para configurar vSphere with Tanzu con NSX-T Data Center 68

Topologías de un clúster supervisor con NSX-T Data Center 75

Consideraciones sobre prácticas recomendadas para configurar el clúster supervisor con NSX-T Data Center 77

Instalar y configurar NSX-T Data Center para vSphere with Tanzu 78

Configurar redes de vSphere y NSX Advanced Load Balancer para vSphere with Tanzu 96

Componentes de NSX Advanced Load Balancer 99

Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y NSX Advanced Load Balancer 100

Topología para clúster supervisor con redes de vSphere y NSX Advanced Load Balancer 107

Instalar y configurar el NSX Advanced Load Balancer 108

Configurar redes de vSphere y el equilibrador de carga de HAProxy para vSphere with Tanzu 123
Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y el equilibrador de carga de HAProxy 124
Topologías para implementar el equilibrador de carga de HAProxy 127
Crear una instancia de vSphere Distributed Switch para un clúster supervisor para su uso con el equilibrador de carga de HAProxy 136
Instalar y configurar el equilibrador de carga de HAProxy 137

5 Configurar y administrar un clúster supervisor 143
Requisitos previos para configurar vSphere with Tanzu en un clúster de vSphere 144
Habilitar la administración de cargas de trabajo con redes de vSphere 147
Habilitar la administración de cargas de trabajo con redes de NSX-T Data Center 155
Asignar la licencia de Tanzu Edition a clúster supervisor 159
Reemplazar el certificado VIP para conectarse de forma segura al endpoint de API de clúster supervisor 159
Integrar servicio Tanzu Kubernetes Grid en el clúster supervisor con Tanzu Mission Control 160
Configurar la CNI predeterminada para los clústeres de Tanzu Kubernetes 162
Agregar redes de cargas de trabajo a un clúster supervisor configurada con redes de VDS 163
Cambiar el tamaño del plano de control de un clúster supervisor 165
Cambiar la configuración de red de administración en un clúster supervisor 165
Cambiar la configuración de red de carga de trabajo en un clúster supervisor configurada con redes de VDS 166
Cambiar la configuración de red de carga de trabajo en un clúster supervisor configurada con NSX-T Data Center 167
Resolución de estados de errores en clúster supervisor durante la configuración inicial o la actualización 168
Configuración de los ajustes del proxy HTTP en vSphere with Tanzu 173
Transmitir registros del plano de control de clúster supervisor a un rsyslog remoto 177

6 Crear y administrar bibliotecas de contenido en vSphere with Tanzu 180
Crear y administrar bibliotecas de contenido para versiones de Tanzu Kubernetes 180
Acerca de las distribuciones de versión de Tanzu Kubernetes 180
Crear, proteger y sincronizar una biblioteca de contenido suscrita para las versiones de Tanzu Kubernetes 181
Crear, proteger y sincronizar una biblioteca de contenido local para versiones de Tanzu Kubernetes 184
Migrar clústeres de Tanzu Kubernetes a una nueva biblioteca de contenido 188
Importar el archivo OVA de HAProxy a una biblioteca de contenido local 189
Crear y administrar bibliotecas de contenido para máquinas virtuales independientes en vSphere with Tanzu 190
Crear una biblioteca de contenido para máquinas virtuales independientes en vSphere with Tanzu 191
Rellenar una biblioteca de contenido con imágenes de máquina virtual para máquinas virtuales independientes en vSphere with Tanzu 193

Asociar una biblioteca de contenido de máquina virtual con un espacio de nombres en vSphere with Tanzu 195
Administrar bibliotecas de contenido de máquina virtual en un espacio de nombres en vSphere with Tanzu 196

7 Configurar y administrar los espacios de nombres de vSphere 198
Creación y configuración de un espacio de nombres de vSphere 198
Establecer reservas y límites de CPU y de memoria predeterminados para los contenedores de pod de vSphere 202
Configurar limitaciones en objetos de Kubernetes en un espacio de nombres de vSphere 203
Supervisar y administrar recursos en un espacio de nombres de vSphere 205
Configurar un espacio de nombres de vSphere para las versiones de Tanzu Kubernetes 205
Agregar directivas de seguridad a un espacio de nombres de clúster supervisor en NSX 208
Crear una directiva de seguridad 208
Aprovisionar una plantilla de espacio de nombres de autoservicio 209
Crear y configurar una plantilla de espacio de nombres de autoservicio 210
Desactivar un espacio de nombres de autoservicio 211
Crear un espacio de nombres de autoservicio 212
Crear un espacio de nombres de autoservicio con anotaciones y etiquetas 213
Actualizar un espacio de nombres de autoservicio mediante la anotación kubectl y la etiqueta kubectl 214
Actualizar un espacio de nombres de autoservicio mediante kubectl edit 216
Eliminar un espacio de nombres de autoservicio 217

8 Administrar servicios de supervisor con vSphere with Tanzu 219
Agregar una instancia de servicio de supervisor a vCenter Server 221
Instalar un servicio de supervisor en clústeres supervisor 223
Acceder a la interfaz de administración de un servicio de supervisor en el clúster supervisor 225
Agregar una nueva versión a un servicio de supervisor 226
Ver servicios de supervisor instalados en un clúster supervisor 226
Desactivar un servicio de supervisor o una versión 227
Activar una versión de servicio de supervisor en vCenter Server 228
Desinstalar servicio de supervisor de clúster supervisor 229
Eliminar una versión del servicio de supervisor 229
Eliminar un servicio de supervisor 230

9 Conectarse a clústeres de vSphere with Tanzu 232
Descargar e instalar Herramientas de la CLI de Kubernetes para vSphere 232
Configurar el inicio de sesión seguro para clústeres de vSphere with Tanzu 235
Conectarse al clúster supervisor como usuario vCenter Single Sign-On 236
Autenticarse con clústeres de Tanzu Kubernetes 237
Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On 238
Conectarse al plano de control del clúster de Tanzu Kubernetes como el administrador 240

Conectarse mediante SSH a nodos de clúster de Tanzu Kubernetes como usuario del sistema con una clave privada 242
Conectarse mediante SSH a nodos de clúster de Tanzu Kubernetes como usuario del sistema con una contraseña 245
Crear una máquina virtual de host de salto de Linux 246
Conceder acceso de desarrollador a clústeres de Tanzu Kubernetes 248

10 Usar almacenamiento persistente en vSphere with Tanzu 250
Cómo se integra vSphere with Tanzu con el almacenamiento de vSphere 255
Funcionalidad admitida por el componente CNS-CSI de vSphere y CSI paravirtual en vSphere with Tanzu 258
Permisos de almacenamiento en vSphere with Tanzu 259
Crear directivas de almacenamiento para vSphere with Tanzu 260
Cambiar la configuración de almacenamiento en el clúster supervisor 263
Cambiar la configuración de almacenamiento en un espacio de nombres 264
Mostrar clases de almacenamiento en un espacio de nombres de vSphere o clúster de Tanzu Kubernetes 264
Aprovisionar un volumen persistente dinámico para una aplicación con estado 266
Aprovisionamiento de un volumen persistente estático en un clúster de Tanzu Kubernetes 268
Crear volúmenes persistentes ReadWriteMany en vSphere with Tanzu 270
Expansión de volúmenes en vSphere with Tanzu 272
Expandir un volumen persistente en modo sin conexión 274
Expandir un volumen persistente en modo en línea 275
Supervisar volúmenes persistentes en vSphere Client 277
Supervisar el estado del volumen en un clúster de espacio de nombres de vSphere o Tanzu Kubernetes 279
Usar la plataforma para la persistencia de datos de vSAN con servicios con estado modernos 281
Etiquetar dispositivos de almacenamiento para vSAN Direct 286
Configurar vSAN Direct para vSphere with Tanzu 293
Habilitar servicios con estado en vSphere with Tanzu 294
Supervisar servicios con estado en vSphere with Tanzu 297
Comprobar las directivas de almacenamiento disponibles para los servicios con estado 299
Crear directiva de almacenamiento SNA vSAN 300
Crear directiva de almacenamiento de vSAN Direct 301

11 Implementar cargas de trabajo en pods de vSphere 303
Obtener y utilizar el contexto del clúster supervisor 303
Implementar una aplicación en un pod de vSphere en un espacio de nombres de vSphere 304
Implementar una aplicación en un pod de vSphere mediante el registro de Harbor integrado 305
Ampliar una aplicación de pod de vSphere 306
Implementar un pod de vSphere confidencial 307

12 Implementar y administrar máquinas virtuales en vSphere with Tanzu 311

Crear una clase de máquina virtual en vSphere with Tanzu 315

Atributos de las clases de máquina virtual en vSphere with Tanzu 318

Agregar dispositivos PCI a una clase de máquina virtual en vSphere with Tanzu 319

Editar o eliminar una clase de máquina virtual en vSphere with Tanzu 322

Asociar una clase de máquina virtual con un espacio de nombres en vSphere with Tanzu 324

Administrar clases de máquinas virtuales en un espacio de nombres en vSphere with Tanzu 325

Ver recursos de máquina virtual disponibles en un espacio de nombres en vSphere with Tanzu 326

Implementar una máquina virtual en vSphere with Tanzu 329

Instalar el controlador invitado de NVIDIA en una máquina virtual en vSphere with Tanzu 333

Supervisar máquinas virtuales disponibles en vSphere with Tanzu 334

13 Aprovisionar y operar clústeres TKGS 336

Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS 336

Clases de máquina virtual para clústeres de Tanzu Kubernetes 343

Aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS 346

Requisitos para usar la API v1alpha2 de TKGS 346

API v1alpha2 de TKGS para aprovisionar clústeres de Tanzu Kubernetes 349

YAML de ejemplo para el aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS 354

Actualizar una versión de Tanzu Kubernetes después de convertir la especificación del clúster a la API v1alpha2 de TKGS 357

Configurar un clúster de Tanzu Kubernetes con una red de pods enrutable mediante la API v1alpha2 362

Parámetros de configuración para la API v1alpha2 de TKGS 364

Ejemplos de configuración de la instancia de TKGS mediante la API de v1alpha2 370

Ampliar un clúster de Tanzu Kubernetes mediante la API v1alpha2 de TKGS 375

Aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha1 de servicio Tanzu Kubernetes Grid 383

Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha1 de servicio Tanzu Kubernetes Grid 384

Parámetros de configuración para clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1 388

Ejemplos del aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1 398

Parámetros de configuración para la API v1alpha1 de servicio Tanzu Kubernetes Grid 408

Ejemplos de configuración de la API de servicio Tanzu Kubernetes Grid v1alpha1 412

Escalar un clúster de Tanzu Kubernetes mediante la API v1alpha1 de servicio Tanzu Kubernetes Grid 417

Eliminar un clúster de Tanzu Kubernetes 424

Especificar un editor de texto predeterminado para Kubectl 426

Operar clústeres de Tanzu Kubernetes 427
Supervisar el estado del clúster de Tanzu Kubernetes mediante kubectl 427
Comprobar la preparación del clúster de Tanzu Kubernetes 428
Ver la jerarquía de recursos completa de un clúster de Tanzu Kubernetes 434
Ver el estado del ciclo de vida de los clústeres de Tanzu Kubernetes 434
Utilizar comandos operativos del clúster de Tanzu Kubernetes 436
Utilizar comandos de redes del clúster de Tanzu Kubernetes 438
Obtener los secretos del clúster de Tanzu Kubernetes 441
Comprobar el estado de la máquina de Tanzu Kubernetes 442
Comprobar el estado del clúster de Tanzu Kubernetes 444
Supervisar el estado del clúster de Tanzu Kubernetes mediante vSphere Client 446

14 Implementar cargas de trabajo y paquetes en clústeres TKGS 448
Implementar cargas de trabajo en clústeres de Tanzu Kubernetes 448
Implementar una carga de trabajo de prueba en un clúster de Tanzu Kubernetes 448
Instalar y ejecutar Octant 450
Ejemplo del servicio del equilibrador de carga de Tanzu Kubernetes 450
Equilibrador de carga de servicio de Tanzu Kubernetes con una dirección IP estática (ejemplo) 452
Ejemplos de equilibrador de carga de servicio de Tanzu Kubernetes para la directiva de tráfico local y rangos de IP de origen 454
Ejemplo de entrada de Tanzu Kubernetes mediante Nginx 456
Ejemplo de clase de almacenamiento de Tanzu Kubernetes 460
Ejemplos de notificación de volumen persistente de Tanzu Kubernetes 461
Tutorial del libro de visitas de Tanzu Kubernetes 462
Archivos YAML de ejemplo para libro de visitas 465
Usar las directivas de seguridad de pods con clústeres de Tanzu Kubernetes 470
Ejemplo de enlaces de funciones para la directiva de seguridad de pods 472
Función de ejemplo para la directiva de seguridad de pods 475
Implementar paquetes TKG en clústeres de Tanzu Kubernetes 476
Descargar el paquete de extensiones TKG v1.3.1 476
Instalar los requisitos previos de las extensiones TKG 477
Implementar y administrar la extensión TKG para el registro de Fluent Bit 482
Implementar y administrar la extensión TKG para la entrada de Contour 490
Implementar y administrar la extensión TKG para la supervisión de Prometheus 500
Implementar y administrar la extensión TKG para la supervisión de Grafana 514
Implementar y administrar la extensión TKG para el registro de Harbor 525
Implementar y administrar la extensión TKG para la detección de servicios de DNS externos 536
Implementar cargas de trabajo de AI/ML en clústeres de Tanzu Kubernetes 541
Acerca de la implementación de cargas de trabajo de AI/ML en clústeres TKGS 542
Flujo de trabajo del administrador de vSphere para implementar cargas de trabajo de AI/ML en clústeres TKGS (vGPU) 543

Flujo de trabajo de operadores de clúster para implementar cargas de trabajo de AI/ML en clústeres TKGS 557
Anexo del administrador de vSphere para implementar cargas de trabajo de AI/ML en clústeres TKGS (vGPU e Instancia dinámica de DirectPath I/O) 565
Anexo de operadores de clúster para implementar cargas de trabajo de AI/ML en clústeres TKGS (DLS) 567

15 Usar un registro de contenedores para cargas de trabajo de vSphere with Tanzu 570
Habilitar el registro de Harbor integrado en el clúster supervisor 571
Iniciar sesión en la consola del registro de Harbor integrado 572
Descargar e instalar el certificado de registro de Harbor integrado 572
Configurar un cliente de Docker con un certificado de registro de Harbor integrado 574
Instalar el complemento auxiliar de credenciales de vSphere Docker y conectarse con el registro 575
Insertar imágenes en el registro de Harbor integrado 577
Purgar imágenes del registro de Harbor integrado 580
Utilizar el registro de Harbor integrado con clústeres de Tanzu Kubernetes 580
Usar un registro de contenedor externo con clústeres de Tanzu Kubernetes 584

16 Trabajar con vSphere Lifecycle Manager 590
Requisitos 590
Habilitar vSphere with Tanzu en un clúster administrado por vSphere Lifecycle Manager 591
Actualizar una instancia de clúster supervisor 591
Agregar hosts a un clúster supervisor 592
Quitar hosts de clúster supervisor 593
Deshabilitar una instancia de Supervisor Cluster 593

17 Actualizar el entorno de vSphere with Tanzu 595
Acerca de las actualizaciones de vSphere with Tanzu 595
Actualización de la topología de red 599
Actualizar la topología de red de NSX-T 603
Actualizar vSphere Distributed Switch 604
Actualizar clúster supervisor mediante una actualización de los espacios de nombres de vSphere 605
Actualización automática de clúster supervisor 606
Actualizar complemento de vSphere para kubectl 607
Comprobar la compatibilidad del clúster de Tanzu Kubernetes para actualizar 607
Actualizar clústeres de Tanzu Kubernetes 608
Actualizar un clúster de Tanzu Kubernetes mediante la actualización de la versión de Tanzu Kubernetes 610
Actualizar un clúster de Tanzu Kubernetes mediante el cambio del objeto VirtualMachineClass 613

Actualizar un clúster de Tanzu Kubernetes mediante el cambio de la clase de almacenamiento 616
Actualizar los clústeres de Tanzu Kubernetes con el método de revisión 618

18 Copia de seguridad y restauración de vSphere with Tanzu 621
Consideraciones para realizar copias de seguridad y restaurar vSphere with Tanzu 621
Instalar y configurar el complemento de Velero para vSphere en el clúster supervisor 623
Realizar copias de seguridad y restaurar pods de vSphere mediante el complemento complemento de Velero para vSphere 635
Instalar y configurar el complemento de Velero para vSphere en un clúster de Tanzu Kubernetes 638
Copia de seguridad y restauración de cargas de trabajo del clúster de Tanzu Kubernetes mediante complemento de Velero para vSphere 642
Instalar y configurar Velero y Restic independientes en un clúster de Tanzu Kubernetes 644
Copia de seguridad y restauración de cargas de trabajo de clúster de Tanzu Kubernetes mediante Restic y Velero independientes 649
Copia de seguridad y restauración de vCenter Server 657
Copia de seguridad y restauración de NSX-T Data Center 658

19 Solucionar problemas en vSphere with Tanzu 659
Prácticas recomendadas y solución de problemas de almacenamiento 659
Usar reglas antiafinidad para máquinas virtuales del plano de control en almacenes de datos que no sean de vSAN 659
La directiva de almacenamiento eliminada de vSphere sigue apareciendo como clase de almacenamiento Kubernetes 661
Usar almacenamiento externo con vSAN Direct 661
Solucionar problemas de redes 663
Registrar vCenter Server en NSX Manager 663
No se puede cambiar la contraseña de NSX Appliance 664
Solucionar problemas de flujos de trabajo con errores e instancias de NSX Edge inestables 664
Recopilar paquetes de soporte para la solución de problemas de NSX-T 665
Recopilar archivos de registro de NSX-T 666
Reiniciar el servicio WCP si cambian la dirección IP, la huella digital o el certificado de administración de NSX-T 666
VDS requerido para el tráfico del nodo de transporte del host 667
Solucionar problemas de NSX Advanced Load Balancer 668
Recopilar paquetes de soporte para la solución de problemas 668
Solucionar problemas de actualización de la topología de red 669
Error en la comprobación previa de la actualización debido a que no hay suficiente capacidad en el equilibrador de carga de Edge 669
Se omitieron espacios de nombres de cargas de trabajo del clúster supervisor durante la actualización 669
Servicio de equilibrador de carga omitido durante la actualización 670
Solucionar problemas de clústeres de Tanzu Kubernetes 670

Recopilar paquete de soporte para clústeres de Tanzu Kubernetes 670
Solucionar errores de conexión de vCenter Single Sign-On 671
Solucionar errores de la biblioteca de contenido suscrita 671
Solucionar errores de la biblioteca de contenido local 672
Solucionar errores de aprovisionamiento de clústeres 672
Solucionar errores de implementación de cargas de trabajo 672
Solucionar errores de clase de máquina virtual 673
Reiniciar un trabajo de actualización con errores del clúster de Tanzu Kubernetes 673
Solución de problemas de administración de cargas de trabajo 674
Recopilar el paquete de soporte para la administración de cargas de trabajo 674
Poner en cola el archivo de registro de administración de cargas de trabajo 675
Solucionar errores de compatibilidad del clúster para habilitar la administración de cargas de trabajo 675
Apagar e iniciar el dominio de carga de trabajo de vSphere with Tanzu 677

Configuración y administración de vSphere with Tanzu

Configuración y administración de vSphere with Tanzu proporciona información sobre cómo configurar y administrar la vSphere with Tanzu mediante vSphere Client. También proporciona información sobre el uso de kubectl para conectarse a los espacios de nombres que se ejecutan en vSphere with Tanzu y ejecutar cargas de trabajo de Kubernetes en espacios de nombres designados.

En *Configuración y administración de vSphere with Tanzu*, se ofrece una descripción general de la arquitectura de la plataforma, así como consideraciones y prácticas recomendadas para configurar el almacenamiento, los recursos informáticos y las redes conforme a los requisitos específicos de vSphere with Tanzu. Proporciona instrucciones para habilitar vSphere with Tanzu en clústeres de vSphere existentes, crear y administrar espacios de nombres y supervisar los clústeres de Tanzu Kubernetes creados mediante el servicio VMware Tanzu™ Kubernetes Grid™.

Esta información también proporciona directrices para establecer una sesión con el plano de control de Kubernetes de vSphere with Tanzu a través de kubectl, ejecutar una aplicación de muestra y crear clústeres de Tanzu Kubernetes mediante el servicio VMware Tanzu™ Kubernetes Grid™.

En VMware, valoramos la inclusión. Para fomentar este principio dentro de nuestra comunidad de clientes, socios y personal interno, creamos contenido con un lenguaje inclusivo.

Audiencia prevista

Configuración y administración de vSphere with Tanzu se elaboró para los administradores de vSphere que deseen habilitar vSphere with Tanzu en vSphere, configurar y proporcionar espacios de nombres a los equipos de desarrollo y operaciones, así como administrar y supervisar las cargas de trabajo de Kubernetes en vSphere. Los administradores de vSphere que deseen usar vSphere with Tanzu deben tener conocimientos básicos sobre contenedores y Kubernetes.

Esta información también está destinada a los ingenieros de desarrollo y operaciones que deseen establecer una sesión con el plano de control de vSphere with Tanzu, ejecutar cargas de trabajo de Kubernetes e implementar clústeres de Kubernetes mediante servicio VMware Tanzu™ Kubernetes Grid™. Además, los desarrolladores que están implementando aplicaciones en la plataforma pueden consultar los ejemplos como guía.

Información actualizada

1

La configuración y la administración de vSphere with Tanzu se actualizan regularmente con información nueva y las correcciones necesarias.

En esta tabla se muestra el historial de actualizaciones de la documentación de *Configuración y administración de vSphere with Tanzu* .

Revisión	Descripción
08 de diciembre de 2022	Se agregó información sobre la directiva de seguridad de red. Consulte Agregar directivas de seguridad a un espacio de nombres de clúster supervisor en NSX.
17 de octubre de 2022	Se corrigió el error ortográfico.
12 de octubre de 2022	■ Se agregó un vínculo para la instalación del paquete de TKG 1.6. Consulte Implementar paquetes TKG en clústeres de Tanzu Kubernetes. ■ Se actualizó la especificación de la API v1alpha2 de TKGS con el tipo de datos (cadena) correcto para nodeDrainTimeout. Consulte API v1alpha2 de TKGS para aprovisionar clústeres de Tanzu Kubernetes. ■ Se actualizaron los archivos YAML de origen de la aplicación del libro de visitas. Consulte Archivos YAML de ejemplo para libro de visitas.
15 de septiembre de 2022	Correcciones de errores menores.
29 de julio de 2022	Se aclaró la declaración sobre el cifrado de secretos en Seguridad de vSphere with Tanzu.
07 de julio de 2022	Se agregó un vínculo a la matriz de interoperabilidad de VMware para comprobar la compatibilidad entre vCenter Server y NSX-T. Consulte Acerca de las actualizaciones de vSphere with Tanzu.
28 de junio de 2022	Se actualizó el tema de apagado e inicio de vSphere with Tanzu con un vínculo al procedimiento más reciente. Consulte Apagar e iniciar el dominio de carga de trabajo de vSphere with Tanzu.
24 de junio de 2022	Se actualizó el procedimiento de creación del espacio de nombres de vSphere. Consulte Creación y configuración de un espacio de nombres de vSphere.
03 de junio de 2022	■ Se actualizó documentación de la extensión DNS externo. Consulte Implementar y administrar la extensión TKG para la detección de servicios de DNS externos. ■ Errores corregidos.
24 de mayo de 2022	Se actualizó Crear volúmenes persistentes ReadWriteMany en vSphere with Tanzu con una declaración de compatibilidad para ReadWriteMany con clústeres de Tanzu Kubernetes.
20 de mayo de 2022	Se actualizó el archivo YAML de ejemplo para libro de visitas al especificar redis:v6.0.5 para la implementación de redis-líder. Consulte Archivos YAML de ejemplo para libro de visitas.

Revisión	Descripción
13 de mayo de 2022	- Se actualizó la documentación para instalar el complemento de Velero para vSphere. Consulte Instalar y configurar el complemento de Velero para vSphere en el clúster supervisor. - Error tipográfico menor solucionado.
06 de mayo de 2022	- Se agregó la nota acerca de que el escalado de los volúmenes del nodo de trabajo del clúster de TKGS elimina los datos de volumen existentes. Consulte Escalar volúmenes de nodos. - Se actualizó el tema de integración de SVC-TMC. Consulte Integrar servicio Tanzu Kubernetes Grid en el clúster supervisor con Tanzu Mission Control. - Se actualizó el flujo de trabajo de aprovisionamiento del clúster de TKGS. Consulte Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS. - Se actualizaron los conceptos de redes TKGS. Consulte Redes de clústeres de servicio Tanzu Kubernetes Grid . - Se corrigieron errores tipográficos y se realizaron modificaciones menores.
21 de abril de 2022	Revisiones menores.
18 de abril de 2022	- Se fortaleció la declaración que recomienda el uso de la clase de máquina virtual garantizada para los clústeres de producción para evitar la contención de recursos y el posible tiempo de inactividad de los clústeres. Consulte Clases de máquina virtual para clústeres de Tanzu Kubernetes y Ver recursos de máquina virtual disponibles en un espacio de nombres en vSphere with Tanzu. - Se agregó una nota sobre cómo tener en cuenta los límites de configuración en un espacio de nombres de vSphere donde los clústeres de Tanzu Kubernetes se aprovisionan con las clases de máquina virtual de mejor esfuerzo. Consulte Configurar limitaciones en objetos de Kubernetes en un espacio de nombres de vSphere.
15 de abril de 2022	- Se agregó una nota a la documentación de aprovisionamiento de TKGS que indica que un clúster aprovisionado con 0 nodos de trabajo/grupos de nodos no tiene asignado ningún servicio de equilibrador de carga. - Se actualizó la documentación de la biblioteca de contenido local. Consulte Crear, proteger y sincronizar una biblioteca de contenido local para versiones de Tanzu Kubernetes. - Se agregó más información sobre la clave de autenticación de inicio de sesión del administrador del sistema. Consulte Implementar el controlador. - Se agregó más información sobre el nombre alternativo del sujeto (SAN). Consulte Asignar un certificado al controlador. - Se aclaró que las clases de almacenamiento vsan-direct y vsan-sna solo pueden ser utilizadas por las aplicaciones en el clúster supervisor, pero no dentro de un clúster de Tanzu Kubernetes. Habilitar servicios con estado en vSphere with Tanzu. - Se agregó información sobre cómo configurar la transmisión remota de los registros del plano de control de clúster supervisor. Consulte Transmitir registros del plano de control de clúster supervisor a un rsyslog remoto.
28 de marzo de 2022	Se agregó información sobre la configuración de un proxy HTTP en el entorno de vSphere with Tanzu. Consulte Configuración de los ajustes del proxy HTTP en vSphere with Tanzu.
18 de marzo de 2022	Errores tipográficos menores solucionados.
04 de marzo de 2022	Se agregó un tema de solución de problemas para las bibliotecas de contenido locales. Consulte Solucionar errores de la biblioteca de contenido local.

Revisión	Descripción
28 de febrero de 2022	■ Se agregó un vínculo para instalar los paquetes de TKG 1.5. Consulte Implementar paquetes TKG en clústeres de Tanzu Kubernetes. ■ Se corrigieron los nombres de las máquinas virtuales del plano de control en los diagramas. Consulte Topologías de un clúster supervisor con NSX-T Data Center. ■ Errores tipográficos menores solucionados.
18 de febrero de 2022	■ Se actualizó Configurar el controlador con un paso para las opciones de configuración cuando DHCP no está habilitado. ■ Se actualizó Asignar un certificado al controlador con un paso para cargar un certificado válido creado previamente. ■ Se actualizaron los requisitos del sistema para indicar que no se admite IPv6. Consulte Capítulo 4 Redes para vSphere with Tanzu. ■ Se actualizaron los requisitos de red para los clústeres de TKGS si se personaliza la configuración de `pods.cidrBlocks` en la especificación del clúster. Consulte Requisitos para usar la API v1alpha2 de TKGS y API v1alpha2 de TKGS para aprovisionar clústeres de Tanzu Kubernetes. ■ Se actualizó la lista de comandos de red de ejemplo para clústeres de TKGS. Consulte Utilizar comandos de redes del clúster de Tanzu Kubernetes.
11 de febrero de 2022	■ Se actualizó Habilitar la administración de cargas de trabajo con redes de vSphere para incluir un vínculo al procedimiento para crear y configurar un espacio de nombres de vSphere como siguiente paso después de la habilitación. ■ Se actualizó Creación y configuración de un espacio de nombres de vSphere para incluir un vínculo para iniciar sesión en clúster supervisor como siguiente paso.
08 de febrero de 2022	■ Se actualizaron los requisitos del sistema para instalar el equilibrador de carga del proxy de HA con una nota que indica que la red de carga de trabajo debe estar en una subred diferente a la red de administración. Consulte Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y el equilibrador de carga de HAProxy.
04 de febrero de 2022	■ Se actualizó Crear volúmenes persistentes ReadWriteMany en vSphere with Tanzu para eliminar las directrices obsoletas para las redes. ■ Se actualizó el Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS con contexto y ejemplos adicionales. ■ Se actualizó el tema Redes del clúster supervisor para corregir un error tipográfico. ■ Se actualizó el tema Actualizar los clústeres de Tanzu Kubernetes con el método de revisión con una advertencia para no utilizar el método `kubectl patch` para actualizar una especificación de clúster para cumplir con la API v1alpah2 de TKGS. ■ Se actualizó Actualizar una versión de Tanzu Kubernetes después de convertir la especificación del clúster a la API v1alpha2 de TKGS con una mención explícita de que se debe utilizar el método `kubectl edit` para realizar esta operación.

Revisión	Descripción
28 de enero de 2022	■ Se actualizó el tema Descargas de la CLI de Kubernetes con capturas de pantalla para facilitar la navegación del usuario. Consulte Descargar e instalar Herramientas de la CLI de Kubernetes para vSphere. ■ Se actualizó el tema de escalado de clústeres de Tanzu Kubernetes con información sobre cómo agregar o cambiar volúmenes de nodos de clúster. Consulte Ampliar un clúster de Tanzu Kubernetes mediante la API v1alpha2 de TKGS. ■ Se actualizó el tema Descargar TKG Extensions 1.3.1 para indicar que debe seleccionar la versión 1.3.1 para ver el manifiesto de las extensiones para su descarga. Consulte Descargar el paquete de extensiones TKG v1.3.1. ■ Se actualizaron los requisitos para el rango de CIDR del pod de vSphere al configurar las redes de vSphere y NSX Advanced Load Balancer para vSphere with Tanzu. Consulte Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y NSX Advanced Load Balancer.
17 de diciembre de 2021	Se actualizó el tema de requisitos previos de la extensión TKG 1.3.1 para describir cómo editar la configuración del controlador Kapp para agregar un servidor proxy. Consulte Instalar los requisitos previos de las extensiones TKG.
10 de diciembre de 2021	■ Se actualizaron los temas de Actualizar clústeres de Tanzu Kubernetes para admitir la Aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS de servicio Tanzu Kubernetes Grid. Consulte también Actualizar una versión de Tanzu Kubernetes después de convertir la especificación del clúster a la API v1alpha2 de TKGS. ■ Se actualizó la documentación de las extensiones TKG para abordar los comentarios de los clientes. Consulte Implementar paquetes TKG en clústeres de Tanzu Kubernetes. ■ Se actualizaron los requisitos y la captura de pantalla de la configuración del proxy de TKGS. Consulte Parámetros de configuración para la API v1alpha2 de TKGS.
24 de noviembre de 2021	Se actualizó la documentación para configurar las redes de vSphere y NSX Advanced Load Balancer para vSphere with Tanzu. Consulte Configurar redes de vSphere y NSX Advanced Load Balancer para vSphere with Tanzu.
05 de noviembre 2021	Se agregó un vínculo para instalar paquetes de TKG 1.4 en los clústeres de Tanzu Kubernetes aprovisionados por el servicio Tanzu Kubernetes Grid. Consulte Implementar paquetes TKG en clústeres de Tanzu Kubernetes.
29 de octubre de 2021	■ Se actualizó la documentación para implementar cargas de trabajo de vGPU en clústeres de TKGS . Consulte Implementar cargas de trabajo de AI/ML en clústeres de Tanzu Kubernetes. ■ Se actualizó la documentación de instalación de complemento de Velero para vSphere. Consulte Instalar y configurar el complemento de Velero para vSphere en el clúster supervisor. ■ Se actualizaron los ejemplos de RBAC. Consulte Ejemplo de enlaces de funciones para la directiva de seguridad de pods. ■ Se actualizaron las redes del clúster supervisor. Consulte Redes del clúster supervisor. ■ Se agregó un aviso de precaución a los temas de requisitos previos de redes y habilitación de la administración de cargas de trabajo que indica que DRS no debe deshabilitarse en clúster supervisor y que deshabilitar DRS podría provocar la interrupción de los clústeres.

Revisión	Descripción
21 de octubre de 2021	■ Se agregó documentación para implementar cargas de trabajo de AI/ML en clústeres TKGS habilitados para vGPU. Consulte Implementar cargas de trabajo de AI/ML en clústeres de Tanzu Kubernetes. ■ Se actualizó Agregar dispositivos PCI a una clase de máquina virtual en vSphere with Tanzu con información sobre la compatibilidad de dispositivos PCI en modo de acceso directo. ■ Se movió la lista de versiones de Tanzu Kubernetes a las notas de la versión dedicadas. Consulte estas notas de la versión para ver toda la información de la versión de Tanzu Kubernetes. ■ Se corrigieron errores tipográficos y errores menores en los documentos.
08 de octubre de 2021	■ Se ha actualizado la versión de versión de Tanzu Kubernetes. Consulte Comprobar la compatibilidad del clúster de Tanzu Kubernetes para actualizar y Aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS. ■ Se agregó el procedimiento para instalar el complemento de Velero para vSphere en un entorno aislado. Para obtener más información, consulte Instalar y configurar el complemento de Velero para vSphere en el clúster supervisor. ■ Se actualizó la información sobre la copia de seguridad y la restauración del clúster supervisor. Para obtener más información, consulte Consideraciones para realizar copias de seguridad y restaurar vSphere with Tanzu. ■ Errores corregidos.
05 de octubre de 2021	Versión inicial.

Conceptos de vSphere with Tanzu

2

Mediante el uso de vSphere with Tanzu, puede convertir un clúster de vSphere en una plataforma para ejecutar cargas de trabajo de Kubernetes en grupos de recursos dedicados. Una vez que vSphere with Tanzu está habilitado en un clúster de vSphere, crea un plano de control de Kubernetes directamente en la capa de hipervisor. A continuación, puede ejecutar los contenedores de Kubernetes implementando los pods de vSphere o bien puede crear clústeres de Kubernetes ascendentes a través de servicio VMware Tanzu™ Kubernetes Grid™ y ejecutar las aplicaciones dentro de estos clústeres.

Este capítulo incluye los siguientes temas:

- ¿Qué es vSphere with Tanzu?
- ¿Qué es un pod de vSphere?
- ¿Qué es un clúster de Tanzu Kubernetes?
- Cuándo utilizar pods de vSphere y clústeres de Tanzu Kubernetes
- Usar máquinas virtuales en vSphere with Tanzu
- Flujos de trabajo y funciones de usuario de vSphere with Tanzu
- ¿Cómo cambia vSphere with Tanzu el entorno de vSphere?
- Licencias para vSphere with Tanzu

¿Qué es vSphere with Tanzu?

Puede usar vSphere with Tanzu para transformar vSphere en una plataforma para ejecutar cargas de trabajo de Kubernetes de forma nativa en la capa de hipervisor. Cuando se habilita en un clúster de vSphere, vSphere with Tanzu proporciona la capacidad de ejecutar cargas de trabajo de Kubernetes directamente en hosts ESXi y para crear clústeres de Kubernetes ascendentes en grupos de recursos dedicados.

Los desafíos de la pila de aplicaciones de hoy

Los sistemas distribuidos actuales se construyen con varios microservicios que normalmente ejecutan una gran cantidad de máquinas virtuales y pods de Kubernetes. Normalmente, una pila que no se basa en una vSphere with Tanzu se compone de un entorno virtual subyacente, con una infraestructura de Kubernetes que se implementa dentro de las máquinas virtuales y los pods de Kubernetes correspondientes que también se ejecutan en estas máquinas virtuales. Tres funciones separadas controlan cada sector de la pila: los desarrolladores de aplicaciones, los administradores de clústeres de Kubernetes y los administradores de vSphere.

Figura 2-1. Pila de aplicaciones de hoy

Carga de trabajo de Kubernetes
Pods
Volúmenes
Servicios
. . .
Desarrollador
Clúster de Kubernetes
Trabajadores
Plano de control
ETCD
. . .
Administrador de clústeres
Entorno virtual
Máquinas virtuales
Redes
Almacenamiento
. . .
Administrador de vSphere

Las diferentes funciones no tienen control ni visibilidad sobre los entornos de las demás:

- Como desarrollador de aplicaciones, puede ejecutar pods de Kubernetes, así como implementar y administrar aplicaciones basadas en Kubernetes. No tiene visibilidad sobre toda la pila que ejecuta cientos de aplicaciones.
- Como ingeniero de Desarrollo y operaciones, solo tiene control sobre la infraestructura de Kubernetes, sin las herramientas para administrar o supervisar el entorno virtual y resolver los problemas relacionados con recursos y otros problemas.
- Como administrador de vSphere, tiene control total sobre el entorno virtual subyacente, pero no tiene visibilidad sobre la infraestructura de Kubernetes, la colocación de los distintos objetos de Kubernetes en el entorno virtual y la forma en que estos consumen los recursos.

Las operaciones en la pila completa pueden ser desafiantes, ya que requieren comunicación entre las tres funciones. La falta de integración entre las diferentes capas de la pila también puede presentar desafíos. Por ejemplo, el programador de Kubernetes no tiene visibilidad sobre el inventario de vCenter Server y no puede colocar los pods de forma inteligente.

¿Cómo ayuda vSphere with Tanzu?

vSphere with Tanzu crea un plano de control de Kubernetes directamente en la capa de hipervisor. Como administrador de vSphere, puede habilitar los clústeres de vSphere existentes para **Administración de cargas de trabajo** y así crear una capa de Kubernetes dentro de los hosts ESXi que forman parte del clúster. Un clúster habilitado con **Administración de cargas de trabajo** se denomina un clúster supervisor.

Figura 2-2. vSphere with Tanzu

Al tener un plano de control de Kubernetes en la capa de hipervisor, se habilitan las siguientes capacidades en vSphere:

- Como administrador de vSphere, puede crear espacios de nombres en el clúster supervisor, denominados espacios de nombres de vSphere, y configurarlos con la cantidad especificada de memoria, CPU y almacenamiento. Puede proporcionar espacios de nombres de vSphere a los ingenieros de desarrollo y operaciones.
- Como ingeniero de desarrollo y operaciones, puede ejecutar cargas de trabajo compuestas por contenedores de Kubernetes en la misma plataforma con grupos de recursos compartidos dentro de un espacio de nombres de vSphere. En vSphere with Tanzu, los contenedores se ejecutan dentro de un tipo especial de máquina virtual denominado pod de vSphere. También puede implementar máquinas virtuales comunes.
- Como ingeniero de desarrollo y operaciones, puede crear y administrar varios clústeres de Kubernetes dentro de un espacio de nombres y administrar su ciclo de vida mediante el servicio Tanzu Kubernetes Grid. A los clústeres de Kubernetes creados mediante el servicio Tanzu Kubernetes Grid se los conoce como Tanzu Kubernetes.

- Como administrador de vSphere, puede administrar y supervisar pods de vSphere, máquinas virtuales y clústeres de Tanzu Kubernetes mediante el uso de vSphere Client.
- Como administrador de vSphere, tiene total visibilidad sobre los pods de vSphere y clústeres de Tanzu Kubernetes que se ejecutan en diferentes espacios de nombres, su colocación en el entorno y la forma en que estos usan recursos.

La ejecución de Kubernetes en la capa de hipervisor también facilita la colaboración entre los administradores de vSphere y los equipos de ingenieros de desarrollo y operaciones, ya que ambas funciones trabajan con los mismos objetos.

¿Qué es una carga de trabajo?

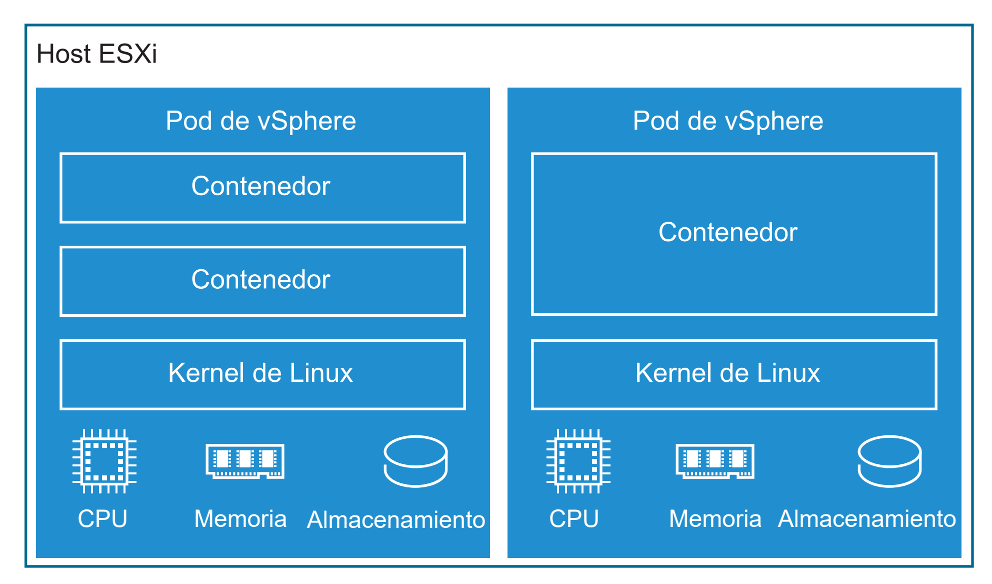
En vSphere with Tanzu, las cargas de trabajo son aplicaciones implementadas de una de las siguientes maneras:

- Las aplicaciones que constan de contenedores que se ejecutan dentro de los pods de vSphere, las máquinas virtuales normales o ambas.
- Clústeres de Tanzu Kubernetes implementados mediante servicio VMware Tanzu™ Kubernetes Grid™.
- Las aplicaciones que se ejecutan dentro de los clústeres de Tanzu Kubernetes que se implementan mediante servicio VMware Tanzu™ Kubernetes Grid™.

¿Qué es un pod de vSphere?

vSphere with Tanzu introduce una nueva construcción llamada pod de vSphere, que equivale a un pod de Kubernetes. Una pod de vSphere es una máquina virtual con un tamaño pequeño que ejecuta uno o más contenedores de Linux. Cada pod de vSphere tiene un tamaño preciso para la carga de trabajo que aloja y tiene reservas de recursos explícitas para esa carga de trabajo. Asigna la cantidad exacta de recursos de almacenamiento, memoria y CPU necesarios para la ejecución de la carga de trabajo. Los pods de vSphere solo se admiten con clústeres supervisor que estén configurados con NSX-T Data Center como pila de redes.

Figura 2-3. pods de vSphere

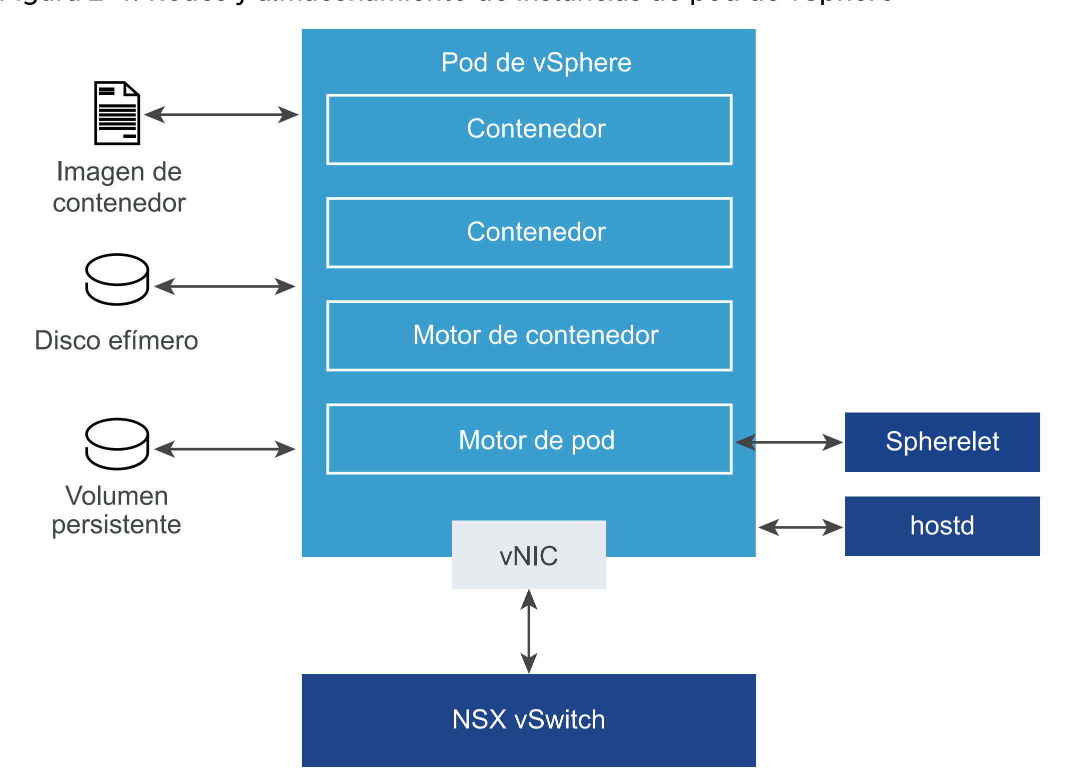


Los pods de vSphere son objetos en vCenter Server y, por lo tanto, habilitan las siguientes capacidades para las cargas de trabajo:

- Aislamiento fuerte. Un pod de vSphere está aislado del mismo modo que una máquina virtual. Cada pod de vSphere tiene su propio kernel único de Linux basado en el kernel utilizado en Photon OS. En lugar de muchos contenedores que comparten un kernel, como en una configuración nativa, en un pod de vSphere, cada contenedor tiene un kernel de Linux único
- Gestión de recursos. vSphere DRS controla la colocación de los pods de vSphere en el clúster supervisor.
- Alto rendimiento. Los pods de vSphere obtienen el mismo nivel de aislamiento de recursos que las máquinas virtuales, lo que elimina los problemas de vecinos ruidosos a la vez que mantiene el tiempo de inicio rápido y una baja sobrecarga de los contenedores.
- Diagnóstico. Como administrador de vSphere, puede utilizar todas las herramientas de introspección y supervisión que están disponibles con vSphere en las cargas de trabajo.

Los pods de vSphere son compatibles con Open Container Initiative (OCI) y pueden ejecutar contenedores desde cualquier sistema operativo, siempre y cuando estos contenedores también sean compatibles con OCI.

Figura 2-4. Redes y almacenamiento de instancias de pod de vSphere



Los pods de vSphere utilizan tres tipos de almacenamiento en función de los objetos que se almacenen; respectivamente, VMDK efímeros, VMDK de volumen persistente y VMDK de imagen de contenedor. Como administrador de vSphere, debe configurar directivas de almacenamiento para la colocación de la memoria caché de imagen de contenedor, los VMDK efímeros y las máquinas virtuales de plano de control en el nivel de clúster supervisor. En un nivel de espacio de nombres de vSphere, se configuran directivas de almacenamiento para la colocación de volúmenes persistentes y la colocación de las máquinas virtuales de los clústeres de Tanzu Kubernetes. Consulte Capítulo 10 Usar almacenamiento persistente en vSphere with Tanzu para obtener más información sobre los requisitos y conceptos de almacenamiento con vSphere with Tanzu.

Para las redes, los pods de vSphere y las máquinas virtuales de los clústeres de Tanzu Kubernetes creados con servicio Tanzu Kubernetes Grid utilizan la topología proporcionada por NSX-T Data Center. Para obtener más información, consulte Redes del clúster supervisor.

Los pods de vSphere solo se admiten en los clústeres supervisor que usan NSX-T Data Center como pila de redes. No son compatibles con los clústeres que están configurados con la pila de redes de vSphere.

¿Qué es un clúster de Tanzu Kubernetes?

Un clúster de Tanzu Kubernetes es una distribución completa de la plataforma de orquestación de contenedores de Kubernetes de código abierto compilada, firmada y compatible con VMware. Los clústeres de Tanzu Kubernetes se pueden aprovisionar y operar en el clúster supervisor

mediante el servicio Tanzu Kubernetes Grid. Un clúster supervisor es un clúster de vSphere para el cual se ha habilitado vSphere with Tanzu.

Características clave de los clústeres de Tanzu Kubernetes creados por el servicio Tanzu Kubernetes Grid

Un clúster de Tanzu Kubernetes aprovisionado por el servicio Tanzu Kubernetes Grid tiene las siguientes características:

- Instalación personalizada de Kubernetes
- Integrado con la infraestructura de vSphere
- Listo para la producción
- Totalmente compatible con VMware
- Administrado por Kubernetes



Nota VMware comercializa un paquete de productos centrados en Kubernetes con la marca Tanzu. Los clústeres de Tanzu Kubernetes que se crean mediante el servicio Tanzu Kubernetes Grid se incluyen en la licencia de Tanzu. Para obtener más información sobre el resto de productos basados en Kubernetes que VMware comercializa con la marca Tanzu, consulte la documentación de VMware Tanzu. Para obtener más información sobre las licencias en vSphere with Tanzu, consulte Licencias para vSphere with Tanzu.

Instalación personalizada de Kubernetes

Un clúster de Tanzu Kubernetes es una instalación personalizada de Kubernetes.

El servicio Tanzu Kubernetes Grid proporciona unos valores predeterminados adaptados y optimizados para que vSphere pueda aprovisionar clústeres de Tanzu Kubernetes. El uso del servicio Tanzu Kubernetes Grid puede ayudarle a reducir la cantidad de tiempo y esfuerzo que suele invertir en implementar y ejecutar un clúster de Kubernetes de nivel empresarial.

Para obtener más información, consulte Arquitectura del servicio Tanzu Kubernetes Grid.

Integrado con la infraestructura de vSphere

Un clúster de Tanzu Kubernetes se integra con la infraestructura subyacente de vSphere, que está optimizada para ejecutar Kubernetes.

Un clúster de Tanzu Kubernetes se integra con la pila de SDDC de vSphere, lo que incluye el almacenamiento, las redes y la autenticación. Asimismo, un clúster de Tanzu Kubernetes se crea sobre una instancia de clúster supervisor asignada a un clúster de vCenter Server. Debido a esta estrecha integración, la ejecución de un clúster de Tanzu Kubernetes resulta una experiencia de producto unificada.

Para obtener más información, consulte Arquitectura de vSphere with Tanzu.

Listo para la producción

Un clúster de Tanzu Kubernetes está optimizado para ejecutar cargas de trabajo de producción.

El servicio Tanzu Kubernetes Grid aprovisiona clústeres de Tanzu Kubernetes que están listos para la producción. Puede ejecutar cargas de trabajo de producción sin necesidad de realizar ninguna configuración adicional. Y, además, puede garantizar su disponibilidad y permitir que se realicen actualizaciones graduales del software de Kubernetes, así como ejecutar diferentes versiones de Kubernetes en clústeres distintos.

Para obtener más información, consulte Capítulo 13 Aprovisionar y operar clústeres TKGS.

Totalmente compatible con VMware

Los clústeres de Tanzu Kubernetes son compatibles con VMware.

Los clústeres de Tanzu Kubernetes usan el sistema operativo Photon OS de VMware (de código abierto y basado en Linux), se implementan en infraestructura de vSphere y se ejecutan en hosts ESXi. Si tiene problemas con cualquiera de las capas de la pila (desde el hipervisor hasta el clúster de Kubernetes), VMware es el único proveedor con el que necesita ponerse en contacto.

Para obtener más información, póngase en contacto con Soporte de VMware.

Administrado por Kubernetes

Los clústeres de Tanzu Kubernetes se administran desde Kubernetes.

Los clústeres de Tanzu Kubernetes se compilan a partir del clúster supervisor, que también es un clúster de Kubernetes. Un clúster de Tanzu Kubernetes se define en el espacio de nombres de vSphere mediante un recurso personalizado. Los clústeres de Tanzu Kubernetes se pueden aprovisionar en función de las necesidades que tenga mediante los comandos habituales de kubectl. Todo el sistema de herramientas mantiene una coherencia: tanto si aprovisiona un clúster como si distribuye cargas de trabajo, utilizará los mismos comandos, el lenguaje YAML habitual y los flujos de trabajo comunes.

Para obtener más información, consulte Modelo de tenant del clúster de Tanzu Kubernetes.

Cuándo utilizar pods de vSphere y clústeres de Tanzu Kubernetes

El uso de varios pods de vSphere o clústeres de Tanzu Kubernetes aprovisionados por servicio Tanzu Kubernetes Grid depende de los objetivos relacionados con la implementación y la administración de las cargas de trabajo de Kubernetes en el clúster supervisor.

Utilice los pods de vSphere si es un administrador de vSphere o un ingeniero de desarrollo y operaciones, y desea hacer lo siguiente:

- Ejecute los contenedores sin necesidad de personalizar un clúster de Kubernetes.
- Crear aplicaciones en contenedor con un fuerte aislamiento de recursos y seguridad.
- Implementar pods de vSphere directamente en hosts ESXi.

Utilice los clústeres de Tanzu Kubernetes aprovisionados por servicio Tanzu Kubernetes Grid si es un desarrollador o ingeniero de desarrollo y operaciones, y desea realizar lo siguiente:

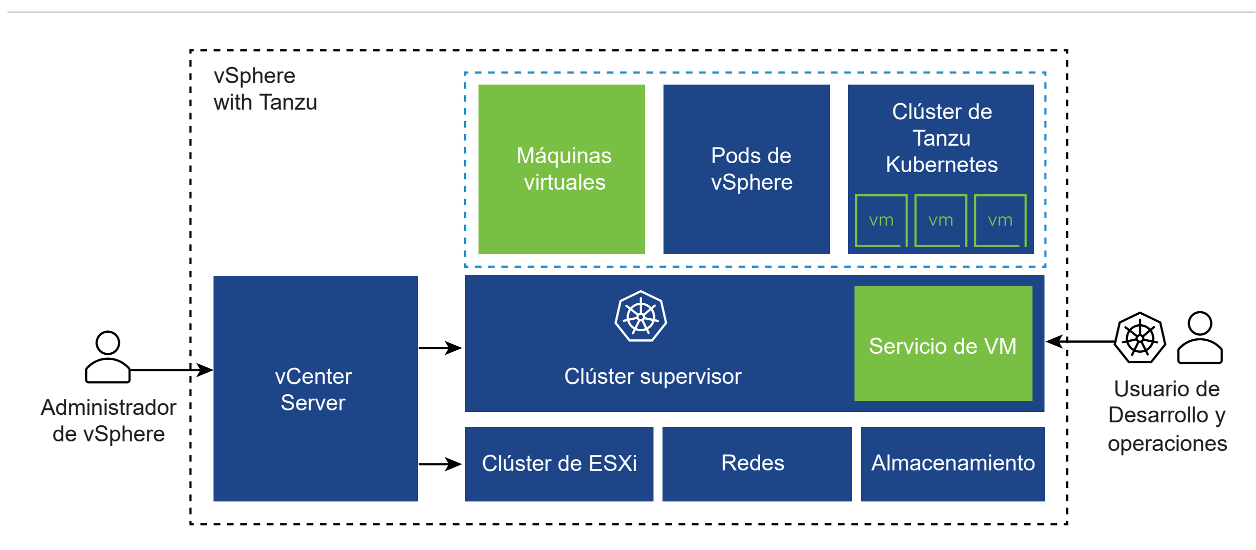
- Ejecutar aplicaciones en contenedor en el software de Kubernetes de código abierto y alineado con la comunidad.
- Controlar el clúster de Kubernetes, incluido el acceso a nivel de la raíz al plano de control y a los nodos de trabajo.
- Estar al día de las versiones de Kubernetes sin necesidad de actualizar la infraestructura.
- Utilizar una canalización de CI/CD para aprovisionar clústeres de Kubernetes de corta duración.
- Personalizar el clúster de Kubernetes; por ejemplo, instalar definiciones de recursos personalizados, operadores y gráficos de Helm.
- Crear espacios de nombres de Kubernetes mediante la CLI de kubectl.
- Administrar el control de acceso de nivel de clúster y configurar `PodSecurityPolicies`.
- Crear servicios de tipo `NodePort`.
- Usar volúmenes de `HostPath` .
- Ejecutar pods con privilegios.

Usar máquinas virtuales en vSphere with Tanzu

vSphere with Tanzu ofrece una funcionalidad de servicio de máquina virtual que permite a los ingenieros de desarrollo y operaciones implementar y ejecutar máquinas virtuales, además de contenedores, en un entorno de Kubernetes común y compartido. Tanto contenedores como máquinas virtuales comparten los mismos recursos de espacio de nombres de vSphere y se pueden administrar a través de una única interfaz de vSphere with Tanzu.

El servicio de máquina virtual responde a las necesidades de los equipos de desarrollo y operaciones que usan Kubernetes, pero tienen cargas de trabajo basadas en máquinas virtuales existentes que no se pueden colocar en contenedores fácilmente. También ayuda a los usuarios a reducir la sobrecarga de administrar una plataforma que no es de Kubernetes junto con una plataforma de contenedor. Al ejecutar contenedores y máquinas virtuales en una plataforma de Kubernetes, los equipos de desarrollo y operaciones pueden consolidar su marca de carga de trabajo en una sola plataforma.

Nota Además de las máquinas virtuales independientes, el servicio de máquina virtual administra las máquinas virtuales que conforman los clústeres de Tanzu Kubernetes. Para obtener información sobre los clústeres, consulte Arquitectura del servicio Tanzu Kubernetes Grid y Capítulo 13 Aprovisionar y operar clústeres TKGS.



Cada máquina virtual implementada a través del servicio de máquina virtual funciona como una máquina completa que ejecuta todos los componentes, incluido su propio sistema operativo, sobre la infraestructura de vSphere with Tanzu. La máquina virtual tiene acceso a las redes y al almacenamiento que proporciona clúster supervisor, y se administra mediante el comando estándar `kubectl` de Kubernetes. La máquina virtual se ejecuta como un sistema completamente aislado que está a prueba de interferencias de otras máquinas virtuales o cargas de trabajo en el entorno de Kubernetes.

¿Cuándo utilizar máquinas virtuales en una plataforma de Kubernetes?

Por lo general, la decisión de ejecutar cargas de trabajo en un contenedor o en una máquina virtual depende de sus necesidades y objetivos empresariales. Entre los motivos para utilizar las máquinas virtuales aparecen los siguientes:

- Las aplicaciones no se pueden poner en contenedores.
- Tiene requisitos de hardware específicos para el proyecto.
- Las aplicaciones están diseñadas para un kernel personalizado o un sistema operativo personalizado.

- Las aplicaciones son más adecuadas para ejecutarse en una máquina virtual.
- Desea tener una experiencia de Kubernetes coherente y evitar la sobrecarga. En lugar de ejecutar conjuntos separados de infraestructura para las plataformas de contenedor y que no son de Kubernetes, puede consolidar estas pilas y administrarlas con un comando de `kubectl` familiar.

Para obtener información sobre la implementación y la administración de máquinas virtuales, consulte Capítulo 12 Implementar y administrar máquinas virtuales en vSphere with Tanzu.

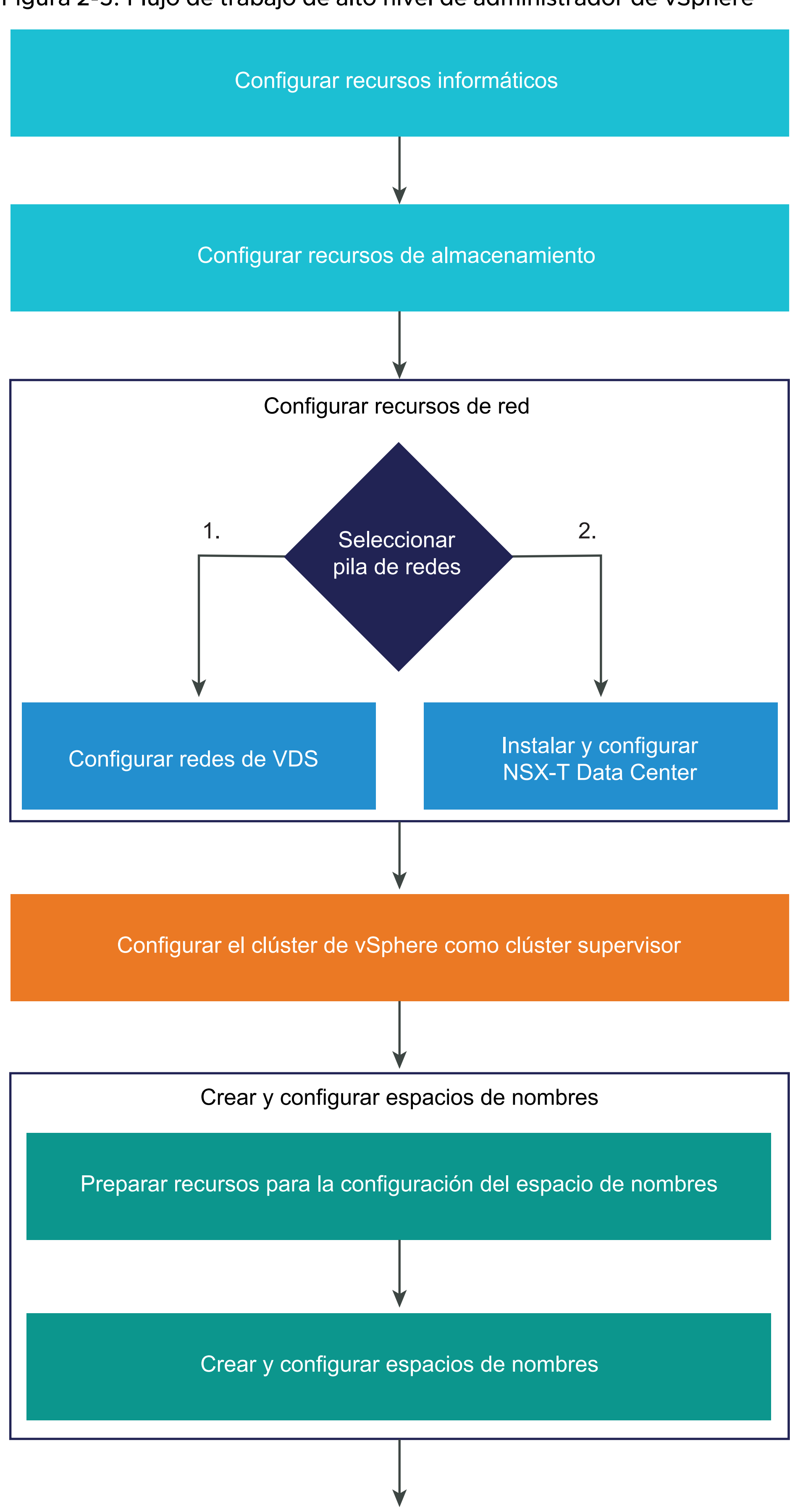
Flujos de trabajo y funciones de usuario de vSphere with Tanzu

La plataforma de vSphere with Tanzu involucra dos funciones: el administrador de vSphere y el ingeniero de desarrollo y operaciones. Ambas funciones interactúan con la plataforma a través de diferentes interfaces y pueden tener usuarios o grupos de usuarios definidos para ellas en vCenter Single Sign-On con permisos asociados. Los flujos de trabajo de las funciones de administrador de vSphere y de ingeniero de desarrollo y operaciones son distintos y se determinan según el área específica de conocimientos que estas requieren.

Flujos de trabajo y funciones de usuario

Como administrador de vSphere, la interfaz principal a través de la cual interactúa con la plataforma de vSphere with Tanzu es vSphere Client. En un nivel alto, sus responsabilidades implican la configuración de una instancia de clúster supervisor y espacios de nombres, donde los ingenieros de desarrollo y operaciones pueden implementar cargas de trabajo de Kubernetes. Debe tener un excelente conocimiento de las tecnologías de vSphere y NSX-T, además de tener un conocimiento básico de Kubernetes.

Figura 2-5. Flujo de trabajo de alto nivel de administrador de vSphere



Como ingeniero de desarrollo y operaciones, puede ser desarrollador de Kubernetes y propietario de aplicaciones, administrador de Kubernetes o una combinación de ambas funciones. Como ingeniero de Desarrollo y operaciones, debe utilizar comandos kubectl para implementar varios pods de vSphere, máquinas virtuales y clústeres de Tanzu Kubernetes en espacios de nombres existentes en el clúster supervisor. Por lo general, como ingeniero de desarrollo y operaciones, no tiene que ser un experto en vSphere y NSX-T, sino que basta con que tenga conocimientos básicos sobre estas tecnologías y la plataforma de vSphere with Tanzu para interactuar con los administradores de vSphere de forma más eficiente.

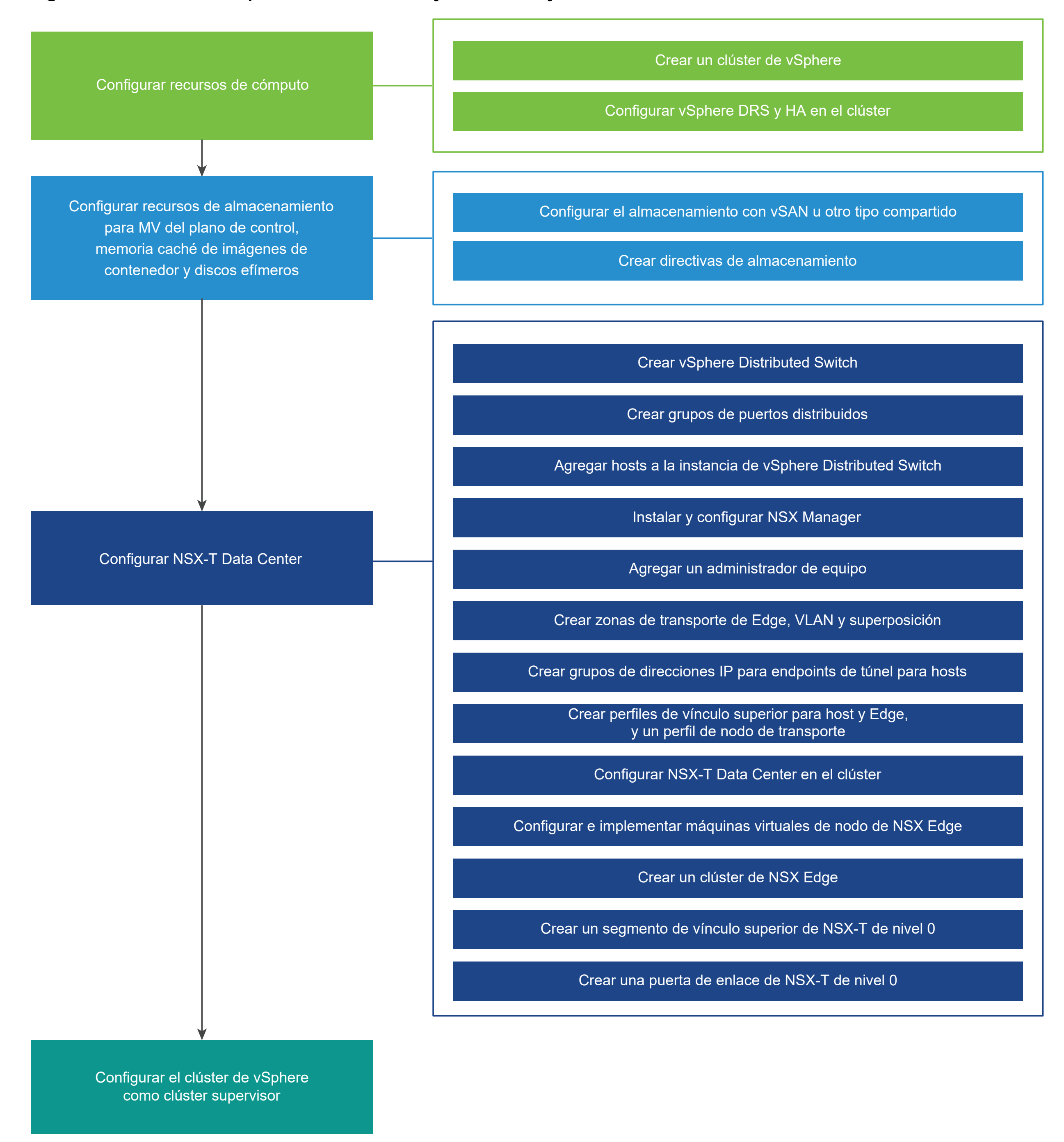
Figura 2-6. Flujo de trabajo de alto nivel de ingeniero de desarrollo y operaciones

Obtener información necesaria del administrador de vSphere
Iniciar sesión en clúster de vSphere y obtener contextos
Implementar cargas de trabajo de Kubernetes
Seleccionar un método
1.
2.
Implementar clústeres de Tanzu Kubernetes
Implementar pods de vSphere y máquinas virtuales

clúster supervisor con el flujo de trabajo de NSX-T Data Center

Como administrador de vSphere, configure la plataforma de vSphere with Tanzu con los componentes de recursos informáticos, almacenamiento y red necesarios. Puede utilizar NSX-T Data Center como la pila de redes para clúster supervisor. Para obtener más información sobre los requisitos del sistema, consulte Requisitos del sistema para configurar vSphere with Tanzu con NSX-T Data Center.

Figura 2-7. clúster supervisor con el flujo de trabajo de redes de NSX-T Data Center



clúster supervisor con el flujo de trabajo de pila de redes de vSphere

Como administrador de vSphere, puede configurar un clúster de vSphere como un clúster supervisor con la pila de redes de vSphere. Para obtener más información sobre los requisitos del sistema, consulte Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y el equilibrador de carga de HAProxy.

Figura 2-8. clúster supervisor con el flujo de trabajo de configuración de la pila de redes de vSphere

Configurar recursos de cómputo

Crear un clúster de vSphere

Configurar vSphere DRS y HA en el clúster

Configurar almacenamiento para las MV del plano de control, la memoria caché de imágenes de contenedor y discos efímeros

Configurar el almacenamiento con vSAN u otro tipo compartido

Crear directivas de almacenamiento

Configurar redes

Crear vSphere Distributed Switch

Agregar los hosts del clúster al conmutador

Crear grupos de puertos distribuidos para redes de carga de trabajo

Instalar y configurar el equilibrador de carga de HAProxy

Crear una biblioteca de contenido suscrita para clústeres de Tanzu Kubernetes

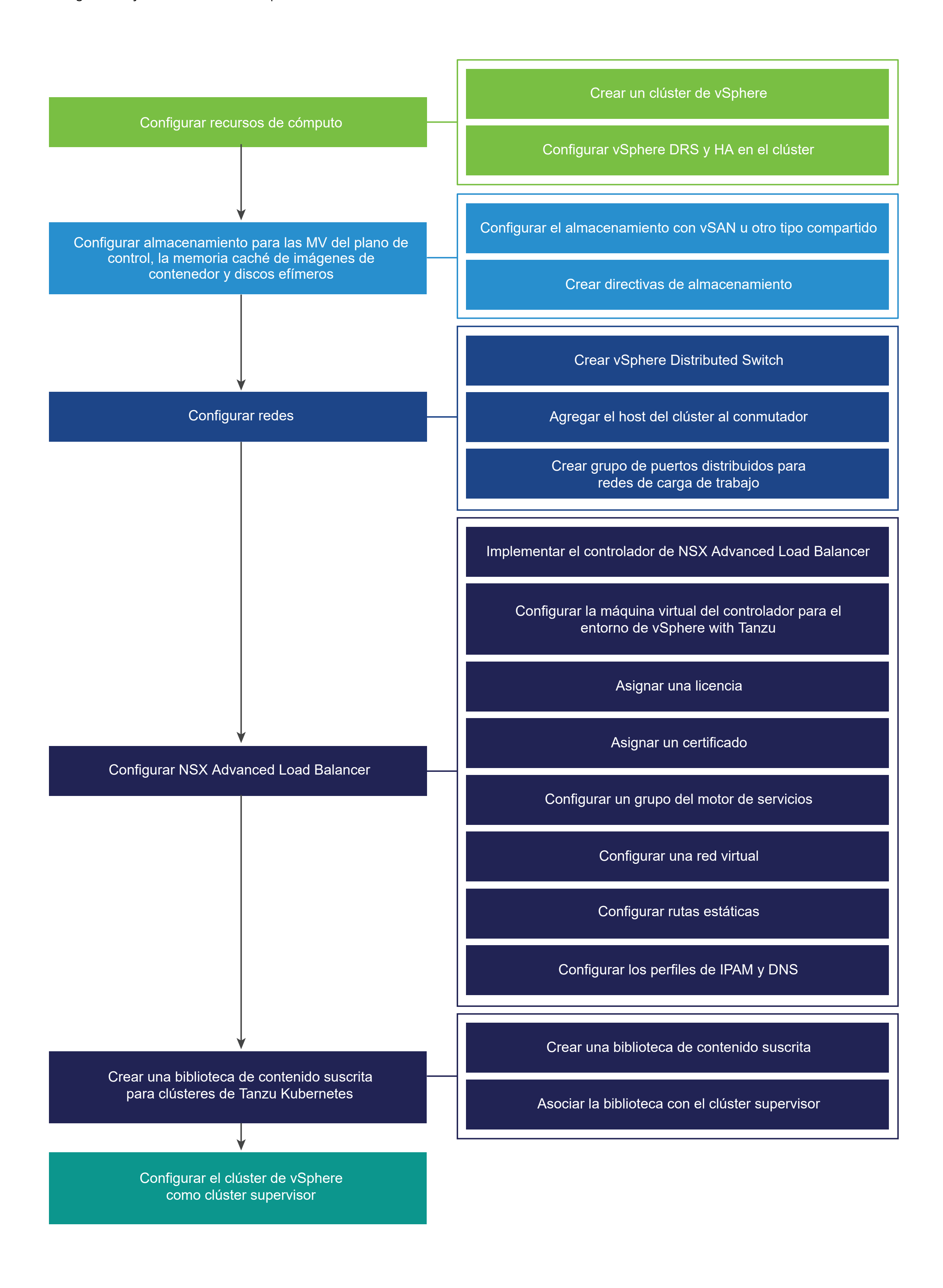
Crear una biblioteca de contenido suscrita

Asociar la biblioteca con el clúster supervisor

Configurar el clúster de vSphere como clúster supervisor

El clúster supervisor con redes de vSphere y el flujo de trabajo de NSX Advanced Load Balancer

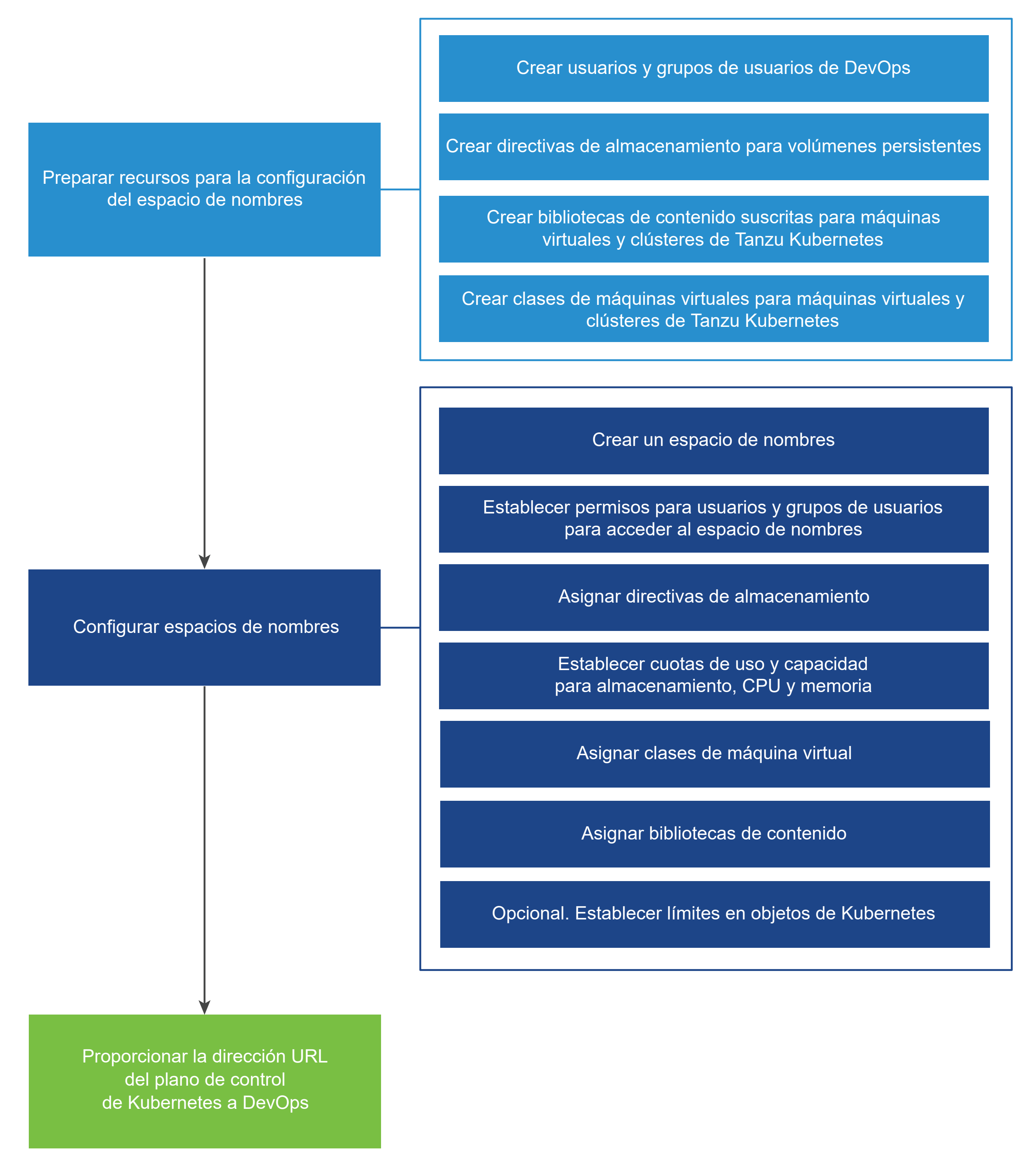
El diagrama muestra el flujo de trabajo para configurar redes de vSphere y NSX Advanced Load Balancer para vSphere with Tanzu. Para obtener más información, consulte Instalar y configurar el NSX Advanced Load Balancer.


Configurar recursos de cómputo
Crear un clúster de vSphere
Configurar vSphere DRS y HA en el clúster
Configurar almacenamiento para las MV del plano de control, la memoria caché de imágenes de contenedor y discos efímeros
Configurar el almacenamiento con vSAN u otro tipo compartido
Crear directivas de almacenamiento
Configurar redes
Crear vSphere Distributed Switch
Agregar el host del clúster al conmutador
Crear grupo de puertos distribuidos para redes de carga de trabajo
Configurar NSX Advanced Load Balancer
Implementar el controlador de NSX Advanced Load Balancer
Configurar la máquina virtual del controlador para el entorno de vSphere with Tanzu
Asignar una licencia
Asignar un certificado
Configurar un grupo del motor de servicios
Configurar una red virtual
Configurar rutas estáticas
Configurar los perfiles de IPAM y DNS
Crear una biblioteca de contenido suscrita para clústeres de Tanzu Kubernetes
Crear una biblioteca de contenido suscrita
Asociar la biblioteca con el clúster supervisor
Configurar el clúster de vSphere como clúster supervisor

Flujo de trabajo de creación y configuración de espacios de nombres

Como administrador de vSphere, debe crear y configurar espacios de nombres en el clúster supervisor. Debe recopilar los requisitos de recursos específicos de los ingenieros de Desarrollo y operaciones para las aplicaciones y cargas de trabajo que desean ejecutar, y configurar los espacios de nombres según corresponda. Para obtener más información, consulte Capítulo 7 Configurar y administrar los espacios de nombres de vSphere.

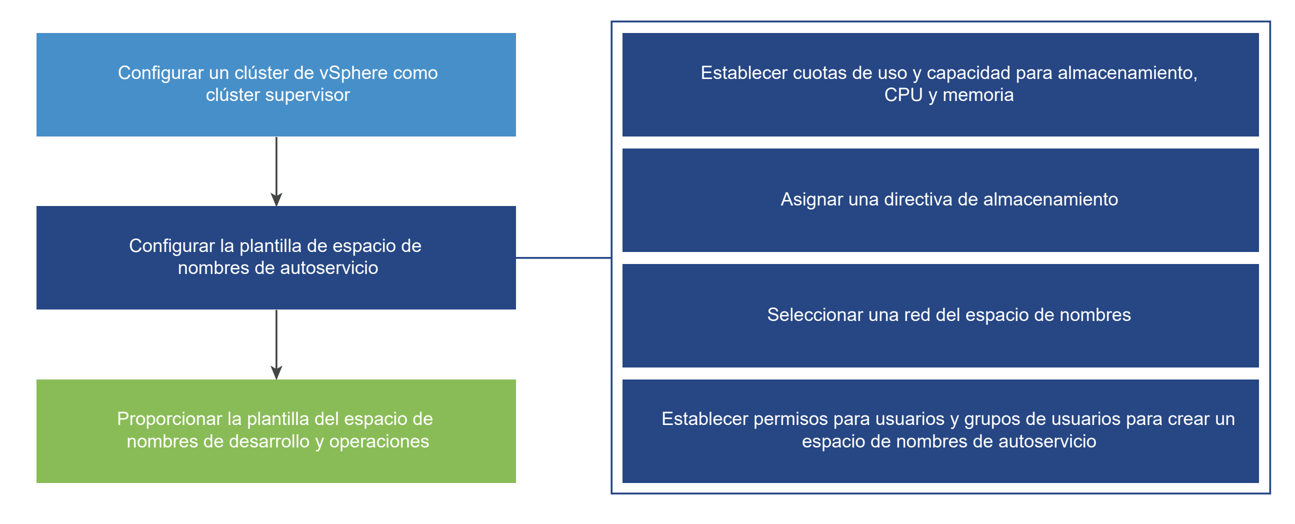
Figura 2-9. Flujo de trabajo de configuración de espacios de nombres



Flujo de trabajo de creación y configuración de espacios de nombres de autoservicio

Como administrador de vSphere, puede crear un espacio de nombres de supervisor, establecer límites de CPU, memoria y almacenamiento en el espacio de nombres, asignar permisos y aprovisionar o activar el servicio de espacio de nombres en un clúster como plantilla.

Figura 2-10. Flujo de trabajo de aprovisionamiento de plantilla de espacio de nombres de autoservicio



Como ingeniero de Desarrollo y operaciones, puede crear un espacio de nombres de supervisor mediante autoservicio e implementar cargas de trabajo dentro de él. Puede compartirlo con otros ingenieros de Desarrollo y operaciones, o eliminarlo cuando ya no sea necesario.

Figura 2-11. Flujo de trabajo de creación de espacio de nombres de autoservicio

Flujos de trabajo de ingeniero de desarrollo y operaciones

Iniciar sesión en el clúster supervisor a través del complemento de CLI kubectl-vsphere

Cambiar a su contexto de Kubernetes funcional

Crear un espacio de nombres de autoservicio en el clúster

Compartir el espacio de nombres con otros ingenieros de desarrollo y operaciones que tengan permisos de propietario

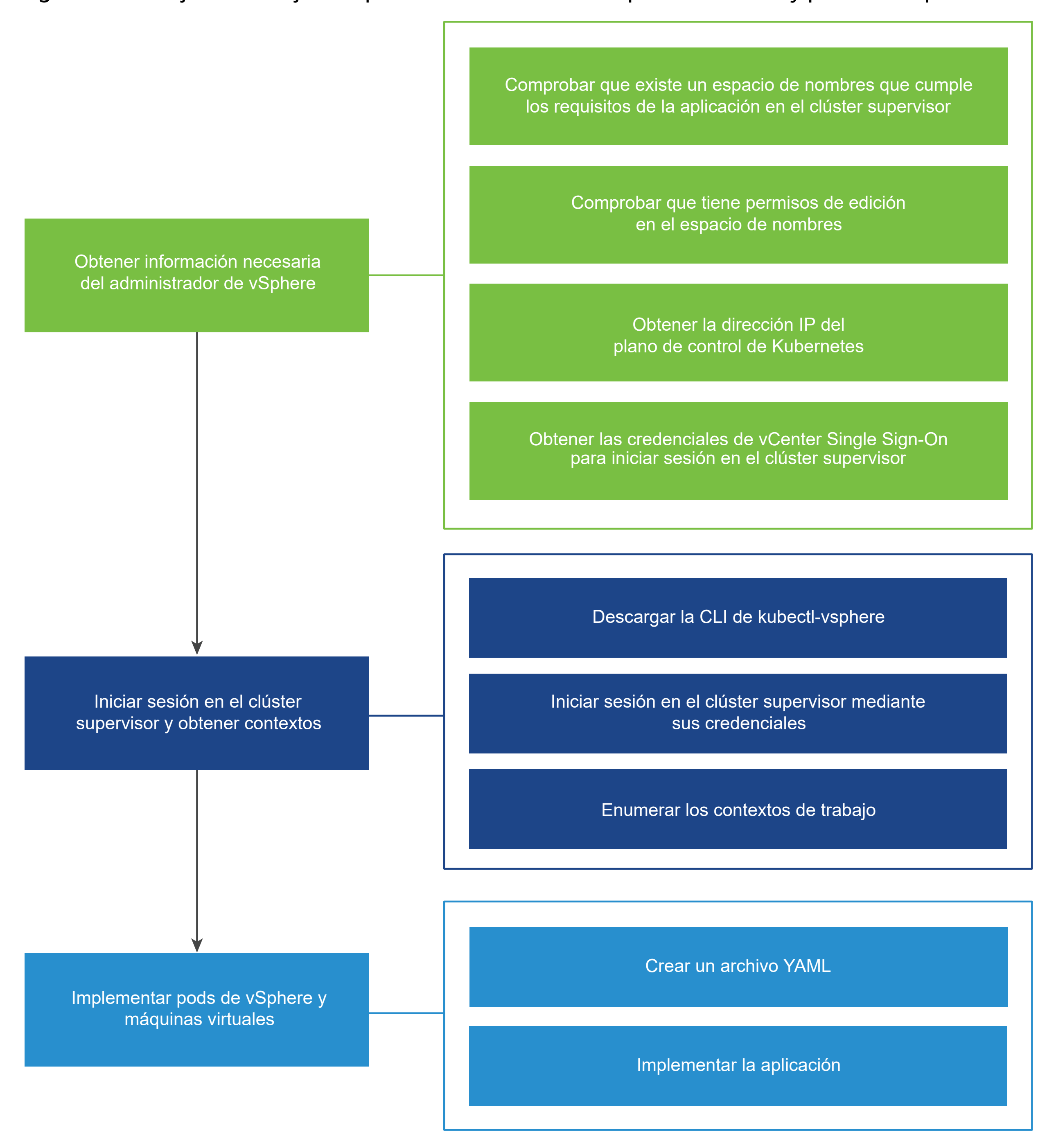
Implementar pods nativos de vSphere o clústeres de Tanzu Kubernetes

Eliminar el espacio de nombres de autoservicio del clúster supervisor

Flujo de trabajo de aprovisionamiento de máquinas virtuales y pod de vSphere

Como ingeniero de Desarrollo y operaciones, puede implementar pods de vSphere y máquinas virtuales dentro de los límites de recursos de un espacio de nombres que se ejecuta en un clúster supervisor. Para obtener más información, consulte Capítulo 11 Implementar cargas de trabajo en pods de vSphere y Capítulo 12 Implementar y administrar máquinas virtuales en vSphere with Tanzu.

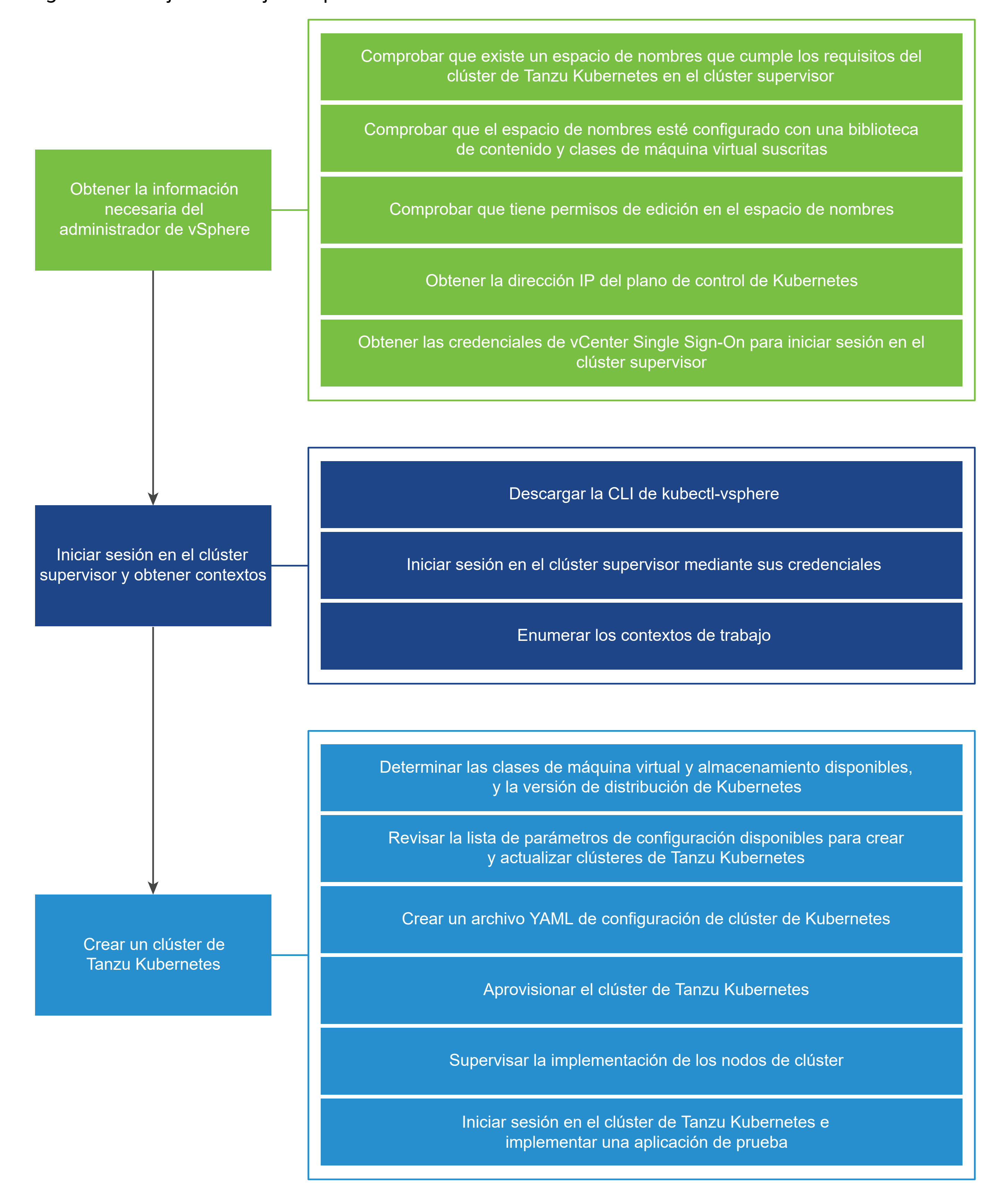
Figura 2-12. Flujo de trabajo de aprovisionamiento de máquinas virtuales y pods de vSphere



Flujo de trabajo de aprovisionamiento del clúster de Tanzu Kubernetes

Como ingeniero de desarrollo y operaciones, debe crear y configurar clústeres de Tanzu Kubernetes en un espacio de nombres creado y configurado por el administrador de vSphere. Para obtener más información, consulte Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS.

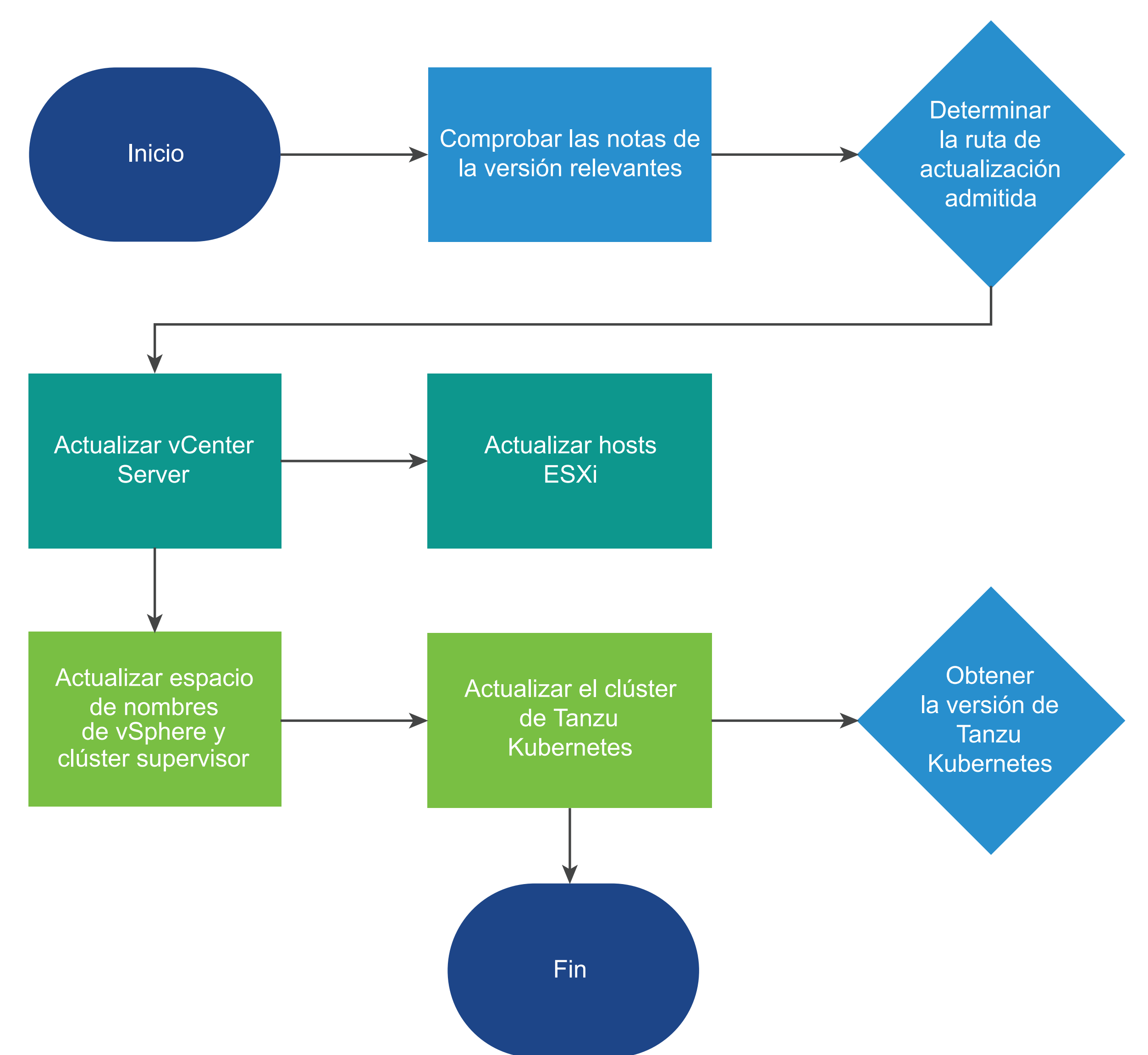
Figura 2-13. Flujo de trabajo de aprovisionamiento del clúster de Tanzu Kubernetes



Flujo de trabajo de actualización de vSphere with Tanzu

En el diagrama se muestra el flujo de trabajo que se utiliza para actualizar el entorno de vSphere with Tanzu, incluidos el clúster supervisor y los clústeres de Tanzu Kubernetes. Para obtener más información, consulte Capítulo 17 Actualizar el entorno de vSphere with Tanzu.

Figura 2-14. Flujo de trabajo de actualización de vSphere with Tanzu



¿Cómo cambia vSphere with Tanzu el entorno de vSphere?

Cuando se configura un clúster de vSphere para las cargas de trabajo de Kubernetes convirtiéndolo, de esta manera, en un clúster supervisor, añade objetos al inventario de vCenter Server, como espacios de nombres, pods de vSphere y clústeres de Tanzu Kubernetes aprovisionados mediante servicio Tanzu Kubernetes Grid.

En cada clúster supervisor, puede ver:

- Espacios de nombres que representan aplicaciones lógicas que se ejecutan en el clúster.
- Grupos de recursos de cada espacio de nombres en clúster supervisor.

En cada espacio de nombres, puede ver:

- pods de vSphere.
- Los clústeres de Kubernetes creados a través del servicio Tanzu Kubernetes Grid.
- Máquinas virtuales de plano de control de Kubernetes.
- Recursos de redes y almacenamiento.
- Permisos de usuario para ese espacio de nombres.

Licencias para vSphere with Tanzu

Una vez que se configura un clúster de vSphere para vSphere with Tanzu y se convierte en una instancia de clúster supervisor, se debe asignar una licencia de Tanzu Edition al clúster antes de que venza el período de evaluación de 60 días.

Acerca de las licencias de Tanzu

Una licencia de Tanzu habilita la funcionalidad de administración de cargas de trabajo vSphere 7.0 Update 1 y posteriores. Se aplica a los clústeres supervisor configurados con la pila de redes de vSphere o con NSX-T Data Center. Para clústeres supervisor que se ejecuten en vSphere 7.0, necesita la licencia de VMware vSphere 7 Enterprise Plus con el complemento para Kubernetes asignada a cada host desde clúster supervisor.

Como administrador de vSphere, cuando asigne una licencia de Tanzu a un clúster supervisor, puede crear y configurar espacios de nombres, y proporcionar acceso a estos espacios de nombres a los ingenieros de desarrollo y operaciones. Como ingeniero de desarrollo y operaciones, puede implementar clústeres de Tanzu Kubernetes y pods de vSphere en los espacios de nombres a los que tiene acceso. Si el clúster supervisor está configurado con la pila de redes de vSphere, solo puede implementar clústeres de Tanzu Kubernetes en ellos.

Licencias de una instancia de clúster supervisor

Después de habilitar **Administración de cargas de trabajo** en un clúster de vSphere, el cual implementa un clúster supervisor, puede utilizar el conjunto completo de funcionalidades del clúster dentro de un período de evaluación de 60 días. Debe asignar una licencia de Tanzu a clúster supervisor antes de que venza el período de evaluación de 60 días.

Si configura NSX-T Data Center como la pila de red de la instancia de clúster supervisor, debe asignar una licencia NSX-T Data Center Advanced o superior a NSX Manager. Si configura clúster supervisor con la pila de redes de vSphere con NSX Advanced Load Balancer, necesitará una licencia adecuada para el equilibrador de carga en función de la edición de la licencia de Tanzu.

Si el entorno se ejecuta sobre vSphere 7.0 y se actualiza clúster supervisor a vSphere 7.0 Update 1 o una versión posterior, el clúster entra en modo de evaluación después de que se complete la actualización. La licencia de VMware vSphere 7 Enterprise Plus with Add-on for Kubernetes que se asigna a los hosts actúa como una licencia regular de vSphere Enterprise 7 Plus. No habilita ninguna funcionalidad de vSphere with Tanzu. En ese caso, debe asignar a la instancia de clúster supervisor una licencia de Tanzu Edition antes de que venza el período de evaluación de 60 días.

Caducidad de la licencia de Tanzu

- vSphere 7.0 Update 3. A partir de vSphere 7.0 Update 3, cuando caduca una licencia de la edición Tanzu, puede seguir usando el conjunto completo de capacidades de vSphere with Tanzu hasta que adquiera nuevas licencias. Sin embargo, no puede asignar la licencia caducada en nuevos clústeres supervisor. Debe asignar una licencia de Tanzu Edition válida a clústeres supervisor recién creados antes de que venza el período de evaluación de 60 días.
- vSphere 7.0 Update 2 y Update 1. Cuando una licencia de Tanzu Edition caduca en un entorno que se ejecuta en vSphere Update 2 o Update 1, como administrador de vSphere no puede crear nuevos espacios de nombres ni actualizar la versión de Kubernetes de clúster supervisor. Como ingeniero de desarrollo y operaciones, no podrá implementar nuevas cargas de trabajo. No se puede cambiar la configuración de los clústeres de Tanzu Kubernetes existentes, como la adición de nodos nuevos.

  Puede seguir implementando cargas de trabajo en clústeres de Tanzu Kubernetes, y todas las cargas de trabajo existentes seguirán funcionando según lo esperado. Todas las cargas de trabajo de Kubernetes que ya se han implementado continúan con su funcionamiento normal.

Conformidad de la licencia de Tanzu

Una clave de licencia de Tanzu tiene una capacidad por CPU de hasta 32 núcleos por CPU, de forma similar a las licencias de host ESXi. Cuando se asigna una licencia de Tanzu a clúster supervisor, la cantidad de capacidad consumida se determina en función del número de CPU físicas en los hosts del clúster y la cantidad de núcleos en cada CPU. Puede asignar una clave de licencia de la edición Tanzu a varios clústeres supervisor a la vez, pero no puede asignar varias claves de licencia a un clúster.

- vSphere 7.0 Update 3. A partir de vSphere 7.0 Update 3, si expande un clúster supervisor agregando nuevos hosts, por ejemplo, y la clave de licencia que asignó al clúster se queda sin capacidad, puede seguir usando la misma clave de licencia. Sin embargo, para seguir cumpliendo con el CLUF, debe adquirir una nueva clave de licencia con capacidad suficiente para cubrir todas las CPU y núcleos del clúster supervisor
- vSphere 7.0 Update 2 y Update 1. Si el entorno de vSphere with Tanzu se ejecuta en vSphere 7.0 Update 2 y Update 1, el número total de CPU en un clúster supervisor no debe superar la cantidad de capacidad de CPU de la licencia de Tanzu Edition que se asigna al clúster.

Caducidad del período de evaluación

Cuando caduca el período de evaluación de una instancia de clúster supervisor, como administrador de vSphere no se pueden crear nuevos espacios de nombres ni actualizar la versión de Kubernetes de la instancia de clúster supervisor. Como ingeniero de desarrollo y operaciones, no puede implementar nuevas cargas de trabajo ni realizar cambios en la configuración de los clústeres de Tanzu Kubernetes existentes, como agregar nodos nuevos.

Puede seguir implementando cargas de trabajo en clústeres de Tanzu Kubernetes, y todas las cargas de trabajo existentes seguirán funcionando según lo esperado. Todas las cargas de trabajo de Kubernetes que ya se han implementado continúan con su funcionamiento normal.

El comportamiento de caducidad del período de evaluación es válido tanto para vSphere 7.0 Update 2 como para Update 3.

Arquitectura y componentes del vSphere with Tanzu

3

Un clúster habilitado con vSphere with Tanzu se denomina clúster supervisor. El clúster se encuentra en la base de vSphere with Tanzu que proporciona los componentes y los recursos necesarios para ejecutar cargas de trabajo que incluyen pods de vSphere, máquinas virtuales y clústeres de Tanzu Kubernetes.

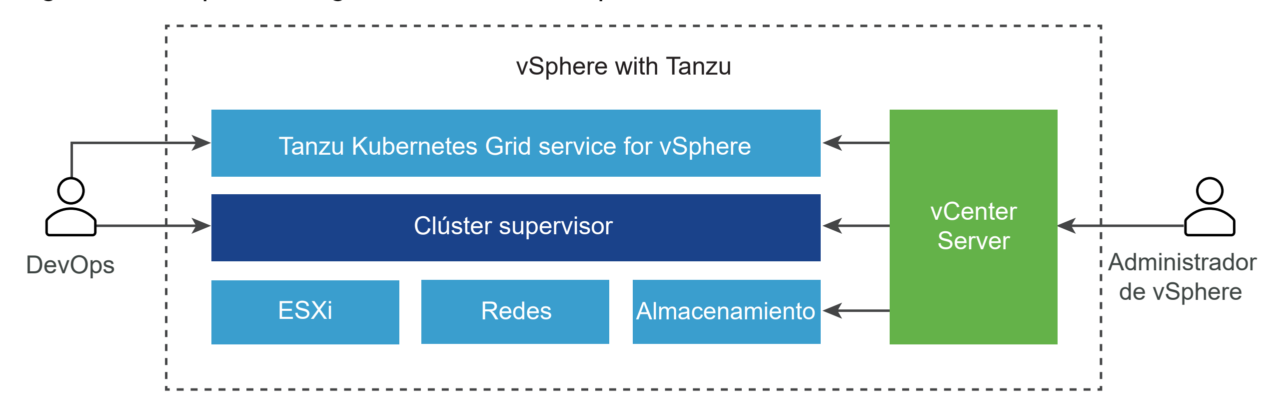
Este capítulo incluye los siguientes temas:

- Arquitectura de vSphere with Tanzu
- Arquitectura del servicio Tanzu Kubernetes Grid
- Modelo de tenant del clúster de Tanzu Kubernetes
- Autenticación de vSphere with Tanzu
- Redes de vSphere with Tanzu
- Seguridad de vSphere with Tanzu
- Almacenamiento de vSphere with Tanzu

Arquitectura de vSphere with Tanzu

Cuando vSphere with Tanzu está habilitado en un clúster de vSphere, crea un plano de control de Kubernetes dentro de la capa de hipervisor. Esta capa contiene objetos específicos que habilitan la capacidad para ejecutar cargas de trabajo de Kubernetes en ESXi.

Figura 3-1. Arquitectura general de clúster supervisor



Un clúster habilitado para vSphere with Tanzu se denomina clúster supervisor. Se ejecuta sobre una capa de SDDC compuesta por ESXi para recursos informáticos, NSX-T Data Center o redes de vSphere, y vSAN u otra solución de almacenamiento compartido. El almacenamiento compartido se utiliza para volúmenes persistentes de los pods de vSphere, máquinas virtuales que se ejecutan dentro del clúster supervisor y pods de un clúster de Tanzu Kubernetes. Después de crear un clúster supervisor, como administrador de vSphere, puede crear espacios de nombres dentro de clúster supervisor que se denominan instancias de espacio de nombres de vSphere. Como ingeniero de Desarrollo y operaciones, puede ejecutar cargas de trabajo compuestas por contenedores que se ejecutan dentro de pods de vSphere y crear clústeres de Tanzu Kubernetes.

Figura 3-2. Arquitectura del clúster supervisor

- Máquina virtual de plano de control de Kubernetes. Se crean tres máquinas virtuales de plano de control de Kubernetes en los hosts que forman parte del clúster supervisor. Las tres máquinas virtuales del plano de control cuentan con equilibrio de carga, ya que cada una de ellas tiene su propia dirección IP. Además, se asigna una dirección IP flotante a una de las máquinas virtuales. vSphere DRS determina la colocación exacta de las máquinas virtuales del plano de control en los hosts ESXi y las migra cuando es necesario. vSphere DRS también se integra con el programador de Kubernetes en las máquinas virtuales del plano de control, por lo que DRS determina la colocación de los pods de vSphere. Cuando programa una pod de vSphere como ingeniero de operaciones y desarrollo, la solicitud pasa por el flujo de trabajo de Kubernetes común y después a DRS, el cual toma la decisión de colocación final.
- Spherelet. Se crea un proceso adicional llamado "Spherelet" en cada host. Se trata de un kubelet que se transporta de forma nativa a ESXi y permite que el host ESXi se convierta en parte del clúster de Kubernetes.

- Container Runtime Executive (CRX). CRX es similar a una máquina virtual desde la perspectiva de Hostd y vCenter Server. CRX incluye un kernel de Linux paravirtualizado que funciona junto con el hipervisor. CRX utiliza las mismas técnicas de virtualización de hardware que las máquinas virtuales y tiene un límite de máquina virtual alrededor. Se utiliza una técnica de arranque directo, que permite que el invitado de CRX de Linux inicie el proceso de inicialización principal sin pasar por la inicialización del kernel. Esto permite que los pods de vSphere arranquen casi tan rápido como los contenedores.
- La API del clúster y servicio VMware Tanzu™ Kubernetes Grid™ son módulos que se ejecutan en clúster supervisor y habilitan el aprovisionamiento y la administración de los clústeres de Tanzu Kubernetes. El módulo servicio de máquina virtual es responsable de implementar y ejecutar las máquinas virtuales independientes y las máquinas virtuales que conforman clústeres de Tanzu Kubernetes.

espacio de nombres de vSphere

Un espacio de nombres de vSphere establece los límites de los recursos donde se pueden ejecutar los pods de vSphere y los clústeres de Tanzu Kubernetes creados mediante servicio Tanzu Kubernetes Grid. Cuando se crea inicialmente, el espacio de nombres tiene recursos ilimitados dentro del clúster supervisor. Como administrador de vSphere, puede establecer límites para la CPU, la memoria y el almacenamiento, así como la cantidad de objetos de Kubernetes que se pueden ejecutar en el espacio de nombres. Se crea un grupo de recursos por cada espacio de nombres en vSphere. Las limitaciones de almacenamiento se representan como cuotas de almacenamiento en Kubernetes.

Figura 3-3. espacio de nombres de vSphere

Clúster supervisor
Espacio de nombres
Pod de vSphere
VM
Pod de vSphere
Clúster de Tanzu Kubernetes
VM
CPU
Memoria
Almacenamiento

Para otorgar acceso a los espacios de nombres al ingeniero de desarrollo y operaciones, como administrador de vSphere, debe asignar permisos a los usuarios o a los grupos de usuarios disponibles en un origen de identidad asociado con vCenter Single Sign-On.

Después de crear un espacio de nombres y configurarlo con límites de recursos y objetos, así como con permisos y directivas de almacenamiento, como ingeniero de desarrollo y operaciones, puede acceder al espacio de nombres para ejecutar cargas de trabajo de Kubernetes y crear clústeres de Tanzu Kubernetes mediante servicio Tanzu Kubernetes Grid.

Clústeres de Tanzu Kubernetes

Un clúster de Tanzu Kubernetes es una distribución completa del software de Kubernetes de código abierto que VMware empaqueta, firma y admite. En el contexto de vSphere with Tanzu, puede utilizar el servicio Tanzu Kubernetes Grid para aprovisionar clústeres de Tanzu Kubernetes en clúster supervisor. Puede invocar a la API del servicio Tanzu Kubernetes Grid de forma declarativa mediante kubectl y una definición de YAML.

Un clúster de Tanzu Kubernetes reside en un espacio de nombres de vSphere. Puede implementar cargas de trabajo y servicios en clústeres de Tanzu Kubernetes de la misma manera y mediante las mismas herramientas que usaría para los clústeres de Kubernetes estándar.

Figura 3-4. Arquitectura de vSphere with Tanzu para clústeres de Tanzu Kubernetes

clúster supervisor configurado con la pila de redes de vSphere

Un clúster supervisor que se configure con la pila de redes de vSphere solo admite la ejecución de clústeres de Tanzu Kubernetes creados mediante el servicio Tanzu Kubernetes Grid. El clúster también es compatible con el servicio de red de vSphere y el servicio de almacenamiento.

Un clúster supervisor que se configura con la pila de redes de vSphere solo admite pods de vSphere. Por lo tanto, el componente Spherelet no está disponible en pods de clúster supervisor y los pods de Kubernetes se ejecutan dentro de clústeres de Tanzu Kubernetes. Un clúster supervisor que se configure con la pila de redes de vSphere tampoco admite el registro de Harbor, ya que el servicio solo se utiliza con los pods de vSphere.

Un espacio de nombres de vSphere creado en un clúster que se configure con la pila de redes de vSphere tampoco admite la ejecución de pods de vSphere, sino solamente de clústeres de Tanzu Kubernetes.

Arquitectura del servicio Tanzu Kubernetes Grid

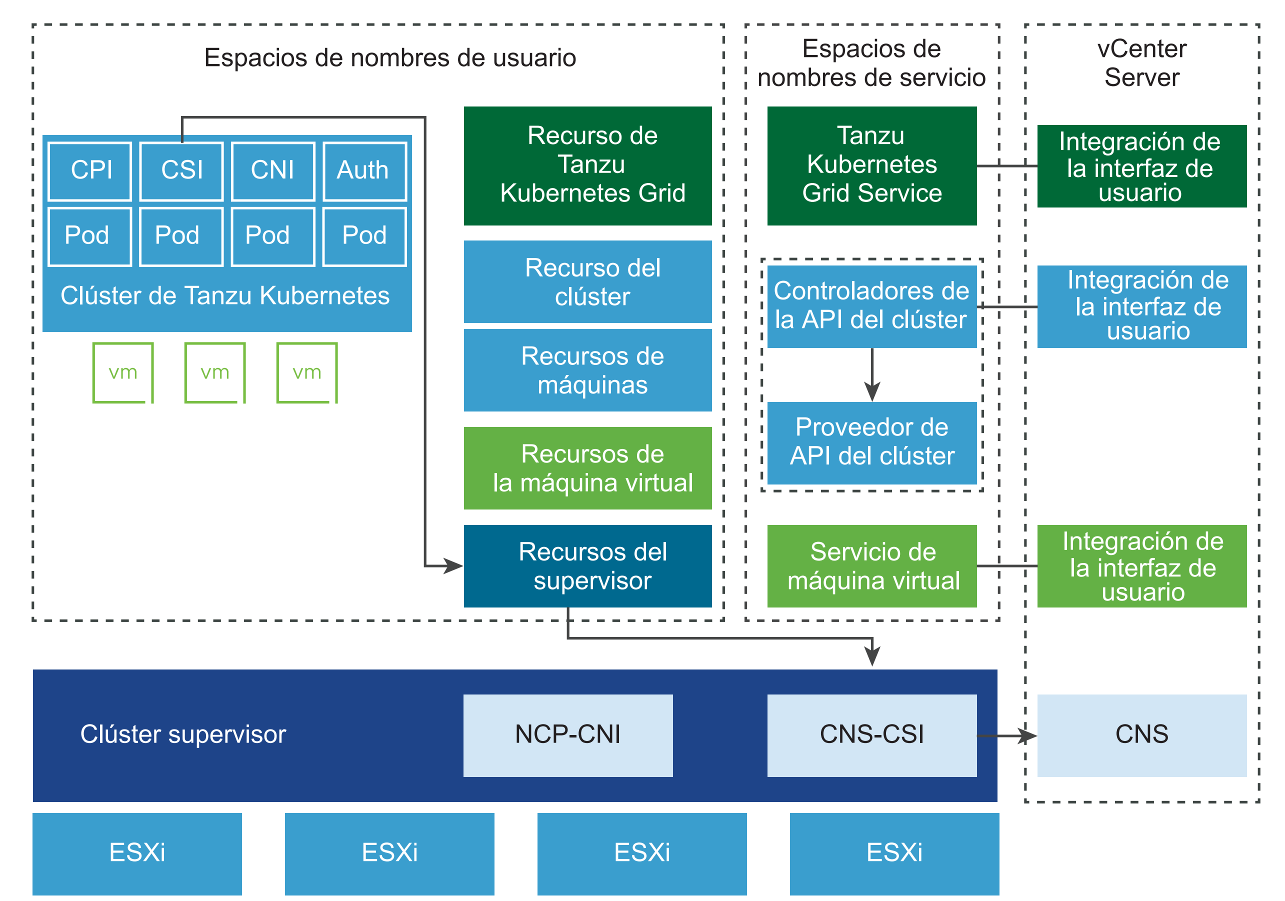
servicio Tanzu Kubernetes Grid proporciona la administración del ciclo de vida de autoservicio de los clústeres de Tanzu Kubernetes. Puede usar servicio Tanzu Kubernetes Grid a fin de crear y administrar los clústeres de Tanzu Kubernetes de una forma declarativa que es conocida para los operadores y los desarrolladores de Kubernetes.

Componentes de servicio Tanzu Kubernetes Grid

servicio Tanzu Kubernetes Grid expone tres capas de controladoras para administrar el ciclo de vida de un clúster de Tanzu Kubernetes.

- servicio Tanzu Kubernetes Grid aprovisiona clústeres que incluyen los componentes necesarios para la integración con los recursos subyacentes de espacio de nombres de vSphere. Estos componentes incluyen un complemento de proveedor de nube que se integra con la instancia de clúster supervisor. Asimismo, un clúster de Tanzu Kubernetes envía solicitudes de volúmenes persistentes a clúster supervisor, que se integra con el almacenamiento nativo en la nube (Cloud Native Storage, CNS) de VMware. Consulte Capítulo 10 Usar almacenamiento persistente en vSphere with Tanzu.
- La API del clúster proporciona API de estilo Kubernetes declarativas para la creación, la configuración y la administración del clúster. Las entradas de la API del clúster incluyen un recurso que describe el clúster, un conjunto de recursos que describen las máquinas virtuales que componen el clúster y un conjunto de recursos que describen los complementos del clúster.
- El servicio de máquina virtual proporciona una API declarativa estilo Kubernetes para la administración de las máquinas virtuales y los recursos de vSphere asociados. El servicio de máquina virtual presenta el concepto de una clase de máquina virtual que representa una configuración de hardware reutilizable y abstracta. La funcionalidad que el servicio de máquina virtual proporciona se utiliza para administrar el ciclo de vida de las máquinas virtuales del plano de control y del nodo de trabajo que alojan un clúster de Tanzu Kubernetes.

Figura 3-5. Arquitectura y componentes del servicio Tanzu Kubernetes Grid



Componentes del clúster de Tanzu Kubernetes

Los componentes que se ejecutan en un clúster de Tanzu Kubernetes abarcan cuatro áreas: autenticación y autorización, integración de almacenamiento, redes de pod, y equilibrio de carga.

- Webhook de autenticación: un webhook que se ejecuta como pod dentro del clúster para validar los tokens de autenticación de usuario.
- Complemento de interfaz de almacenamiento de contenedor: un complemento de CSI paravirtual que se integra con CNS a través de clúster supervisor.
- Complemento de interfaz de redes de contenedor: un complemento de CNI que proporciona redes de pod.
- Implementación de proveedor de nube: admite la creación de servicios de equilibrador de carga de Kubernetes.

API de servicio Tanzu Kubernetes Grid

Use la API de servicio Tanzu Kubernetes Grid para aprovisionar y administrar clústeres de Tanzu Kubernetes. Se trata de una API declarativa que se invoca mediante kubectl y YAML.

Con una API declarativa, en lugar de enviar comandos imperativos al sistema, se especifica el estado deseado del clúster de Tanzu Kubernetes: la cantidad de nodos, el almacenamiento disponible, los tamaños de máquina virtual y la versión de software de Kubernetes. servicio Tanzu Kubernetes Grid se encarga de aprovisionar un clúster que coincide con el estado deseado.

Para llamar a la API de servicio Tanzu Kubernetes Grid, debe invocar kubectl mediante un archivo YAML que, a su vez, invoca la API. Después de crear el clúster, debe actualizar el archivo YAML para actualizar el clúster.

Interfaces de servicio Tanzu Kubernetes Grid

Los administradores de vSphere utilizan vSphere Client para configurar el espacio de nombres de vSphere y conceder permisos. También pueden supervisar los recursos utilizados por los componentes del clúster y ver la información relevante de esos recursos en el inventario de vSphere.

Los ingenieros de desarrollo y operaciones utilizan el complemento de vSphere para kubectl para conectarse a espacio de nombres de vSphere con sus credenciales de vCenter Single Sign-On. Después de conectarse, los ingenieros de desarrollo y operaciones usan kubectl para aprovisionar clústeres de Tanzu Kubernetes.

Los desarrolladores pueden conectarse a un clúster aprovisionado con el complemento de vSphere para kubectl y sus credenciales de vCenter Single Sign-On. Opcionalmente, si el administrador de clústeres configuró un proveedor de autenticación de Kubernetes compatible, los desarrolladores pueden conectarse mediante kubectl. Los desarrolladores utilizan kubectl para implementar cargas de trabajo en Kubernetes e interactuar con el entorno de clústeres.

Demostración de servicio Tanzu Kubernetes Grid

Mire el siguiente video y aprenda a utilizar servicio Tanzu Kubernetes Grid para crear y usar clústeres de Tanzu Kubernetes: vSphere 7 with Kubernetes: Descripción técnica del clúster de Tanzu Kubernetes.

Modelo de tenant del clúster de Tanzu Kubernetes

clúster supervisor es el plano de administración de los clústeres de Tanzu Kubernetes que aprovisiona servicio Tanzu Kubernetes Grid. El modelo de tenant se aplica mediante un espacio de nombres de vSphere en el que residen los clústeres de Tanzu Kubernetes.

Clúster supervisor

clúster supervisor proporciona la capa de administración en la que se compilan los clústeres de Tanzu Kubernetes. servicio Tanzu Kubernetes Grid es un administrador de controladoras personalizado con un conjunto de controladoras que forma parte de clúster supervisor. El propósito de servicio Tanzu Kubernetes Grid es aprovisionar a los clústeres de Tanzu Kubernetes.

Mientras que existe una relación uno a uno entre clúster supervisor y el clúster de vSphere, la relación entre clúster supervisor y los clústeres de Tanzu Kubernetes es del tipo uno a varios. Puede aprovisionar varios clústeres de Tanzu Kubernetes dentro de una única instancia de clúster supervisor. La funcionalidad de administración de cargas de trabajo que ofrece clúster supervisor le permite controlar la configuración y el ciclo de vida del clúster, a la vez que puede mantener la simultaneidad con los elementos de Kubernetes ascendentes.

Para obtener más información, consulte Capítulo 5 Configurar y administrar un clúster supervisor.

Espacio de nombres de vSphere

Puede implementar uno o varios clústeres de Tanzu Kubernetes en un espacio de nombres de vSphere. Las cuotas de recursos y la directiva de almacenamiento se aplican a un espacio de nombres de vSphere y las heredan los clústeres de Tanzu Kubernetes que se implementen allí.

Cuando se aprovisiona un clúster de Tanzu Kubernetes, se crea un grupo de recursos y una carpeta de máquina virtual en el espacio de nombres de vSphere. El plano de control del clúster de Tanzu Kubernetes y las máquinas virtuales del nodo de trabajo se colocan dentro de este grupo de recursos y la carpeta de máquina virtual. Si utiliza vSphere Client, podrá ver esta jerarquía al seleccionar la perspectiva **Hosts y clústeres** y al seleccionar la vista **Máquinas virtuales y plantillas**.

Para obtener más información, consulte Capítulo 7 Configurar y administrar los espacios de nombres de vSphere.

Biblioteca de contenido

Una biblioteca de contenido de vSphere proporciona la plantilla de máquina virtual que se utiliza para crear los nodos de clúster de Tanzu Kubernetes. Para cada clúster supervisor donde pretenda implementar un clúster de Tanzu Kubernetes, debe definir un objeto de biblioteca de contenido suscrita que origine los archivos OVA que utilice servicio Tanzu Kubernetes Grid para compilar los nodos del clúster. Se puede configurar la misma biblioteca de contenido suscrita para varios clústeres supervisor. No hay ninguna relación entre la biblioteca de contenido suscrita y el espacio de nombres de vSphere. La biblioteca de contenido suscrita descarga las plantillas más recientes directamente desde VMware. Cargue las plantillas de OVA que desea utilizar en una biblioteca de contenido local.

Para obtener más información, consulte Crear y administrar bibliotecas de contenido para versiones de Tanzu Kubernetes.

Autenticación de vSphere with Tanzu

Como administrador de vSphere, necesita privilegios para configurar un clúster supervisor y administrar los espacios de nombres. Defina los permisos en los espacios de nombres para determinar qué ingenieros de Desarrollo y operaciones pueden acceder a ellos. Los ingenieros de desarrollo y operaciones se autentican con clúster supervisor mediante las credenciales de vCenter Single Sign-On y únicamente pueden acceder a los espacios de nombres para los que tiene permisos.

Permisos para administradores de vSphere

Como administrador de vSphere, necesita permisos en los clústeres de vSphere para configurarlos como clústeres supervisor, así como para crear y administrar espacios de nombres. Debe tener al menos uno de los siguientes privilegios asociados con sus cuentas de usuario en un clúster de vSphere:

- **Modificar configuración de espacio de nombres**. Le permite crear y configurar espacios de nombres en un clúster supervisor.
- **Modificar configuración de todo el clúster**. Le permite configurar un clúster de vSphere como un clúster supervisor.

Configurar permisos para ingenieros de desarrollo y operaciones

Los administradores de vSphere pueden conceder permisos de vista, edición o propietario a las cuentas de usuario en el nivel del espacio de nombres. Las cuentas de usuario deben estar disponibles en un origen de identidad conectado a vCenter Single Sign-On. Una cuenta de usuario puede tener acceso a varios espacios de nombres a la vez. Los usuarios que pertenecen a los grupos de administradores pueden acceder a todos los espacios de nombres en clúster supervisor.

Tras configurar un espacio de nombres con permisos, cuotas de recursos y almacenamiento, debe proporcionar la URL del plano de control de Kubernetes a los ingenieros de desarrollo y operaciones, quienes la utilizan para iniciar sesión en el plano de control. Una vez iniciada la sesión, los ingenieros de desarrollo y operaciones pueden acceder a todos los espacios de nombres para los que tienen permisos en todos los clústeres supervisor que pertenecen a un sistema vCenter Server. Cuando los sistemas vCenter Server se encuentran en Enhanced Linked Mode, los ingenieros de desarrollo y operaciones pueden acceder a todos los espacios de nombres para los que tienen permisos en todos los clústeres supervisor disponibles en el grupo de Linked Mode. La dirección IP del plano de control de Kubernetes es una dirección IP virtual generada por NSX-T o un equilibrador de carga en el caso de las redes de VDS para que actúe como punto de acceso al plano de control de Kubernetes.

Los ingenieros de desarrollo y operaciones con permisos de propietario pueden implementar cargas de trabajo. Pueden compartir el espacio de nombres con otros ingenieros o grupos de desarrollo y operaciones, o eliminarlo cuando ya no sea necesario. Cuando los ingenieros de desarrollo y operaciones comparten el espacio de nombres, pueden asignar permisos de vista, edición o propietario a otros ingenieros y grupos de desarrollo y operaciones.

Autenticación con el clúster supervisor

Los ingenieros de desarrollo y operaciones utilizan Herramientas de la CLI de Kubernetes para vSphere para autenticarse en clúster supervisor mediante las credenciales de vCenter Single Sign-On y la dirección IP del plano de control de Kubernetes. Para obtener más información, consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

Cuando haya iniciado sesión en clúster supervisor, un proxy de autenticación redirige la solicitud a vCenter Single Sign-On. El complemento kubectl de vSphere establece una sesión con vCenter Server y obtiene un token de autenticación de vCenter Single Sign-On. También obtiene una lista de los espacios de nombres a los que tiene acceso y rellena la configuración con estos espacios de nombres. La lista de espacios de nombres se actualiza en el próximo inicio de sesión si hay cambios en los permisos de su cuenta de usuario.

La cuenta que utiliza para iniciar sesión en el clúster supervisor proporciona acceso solo a los espacios de nombres que se le asignan. No puede iniciar sesión en vCenter Server con esa cuenta. Para iniciar sesión en vCenter Server, necesitará permisos explícitos.

Nota La sesión de kubectl dura 10 horas. Después de que caduque la sesión, debe volver a autenticarse con clúster supervisor. Al cerrar sesión, el token se elimina del archivo de configuración de su cuenta de usuario, pero sigue siendo válido hasta que finalice la sesión.

Autenticarse con clústeres de Tanzu Kubernetes

Los usuarios del clúster de Tanzu Kubernetes (incluidos los desarrolladores, los administradores y los ingenieros de desarrollo y operaciones) pueden autenticarse con un clúster de varias maneras. Para obtener más información, consulte Autenticarse con clústeres de Tanzu Kubernetes.

Nota Los clústeres de Tanzu Kubernetes requieren que las cuentas del usuario y del sistema cuenten con una directiva de seguridad de pods para implementar pods y recursos en un clúster. Para obtener más información, consulte Usar las directivas de seguridad de pods con clústeres de Tanzu Kubernetes.

Redes de vSphere with Tanzu

Un clúster supervisor puede utilizar la pila de redes de vSphere o VMware NSX-T™ Data Center para proporcionar conectividad a las máquinas virtuales, los servicios y las cargas de trabajo del plano de control de Kubernetes. Las redes que se utilizan para los clústeres de Tanzu Kubernetes aprovisionadas por servicio Tanzu Kubernetes Grid son una combinación del tejido que se encuentra subyacente a la infraestructura de vSphere with Tanzu y el software de código abierto que proporciona las redes para los pods, los servicios y las entradas del clúster.

Para obtener más información, consulte Capítulo 4 Redes para vSphere with Tanzu

Seguridad de vSphere with Tanzu

vSphere with Tanzu aprovecha las funciones de seguridad de vSphere y aprovisiona los clústeres de Tanzu Kubernetes que sean seguros de forma predeterminada.

vSphere with Tanzu es un módulo complementario para vSphere que puede aprovechar las funciones de seguridad integradas en vCenter Server y ESXi. Para obtener más información, consulte la documentación de Seguridad de vSphere.

clúster supervisor cifra todos los secretos almacenados en la base de datos (etcd). Los secretos se cifran a través de un archivo de clave de descifrado local, que vCenter Server proporciona en el arranque. La clave de descifrado se almacena en la memoria (tempfs) en los nodos de clúster supervisor y en el disco de forma cifrada dentro de la base de datos de vCenter Server. La clave está disponible en texto no cifrado para los usuarios raíz de cada sistema. Los secretos que se encuentran en la base de datos de cada clúster de carga de trabajo se almacenan en texto no cifrado. Todas las conexiones etcd se autentican con certificados que se generan en la instalación y se rotan durante las actualizaciones. Actualmente no es posible rotar o actualizar manualmente los certificados.

A partir vSphere 7.0 Update 2, puede ejecutar pods de vSphere confidenciales en un clúster supervisor en sistemas AMD. Puede crear pods de vSphere confidenciales agregando el estado de cifrado SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES) como una mejora de seguridad. Para obtener más información, consulte Implementar un pod de vSphere confidencial.

Un clúster de Tanzu Kubernetes está protegido de forma predeterminada. La instancia restrictiva de PodSecurityPolicy (PSP) está disponible para cualquier clúster de Tanzu Kubernetes que aprovisione servicio Tanzu Kubernetes Grid. Si los desarrolladores necesitan ejecutar contenedores raíz o pods con privilegios, al menos un administrador de clústeres deberá crear un objeto RoleBinding que otorgue acceso de usuario a la PSP con privilegios predeterminada. Para obtener más información, consulte Usar las directivas de seguridad de pods con clústeres de Tanzu Kubernetes.

Un clúster de Tanzu Kubernetes no tiene credenciales de infraestructura. Las credenciales que se almacenan en un clúster de Tanzu Kubernetes solo son suficientes para acceder al espacio de nombres de vSphere donde el clúster de Tanzu Kubernetes es tenant. Por ello, no existe la posibilidad de realizar la escalación de privilegios para los operadores de clústeres ni los usuarios.

Los tokens de autenticación que se utilizan para acceder a los clústeres de Tanzu Kubernetes se incluyen en el ámbito de manera que no se pueden utilizar para acceder al clúster supervisor. De este modo, se evita que los operadores del clúster, o los individuos que puedan intentar poner en peligro un clúster, utilicen el acceso de nivel raíz para capturar un token de administrador de vSphere cuando inicien sesión en un clúster de Tanzu Kubernetes.

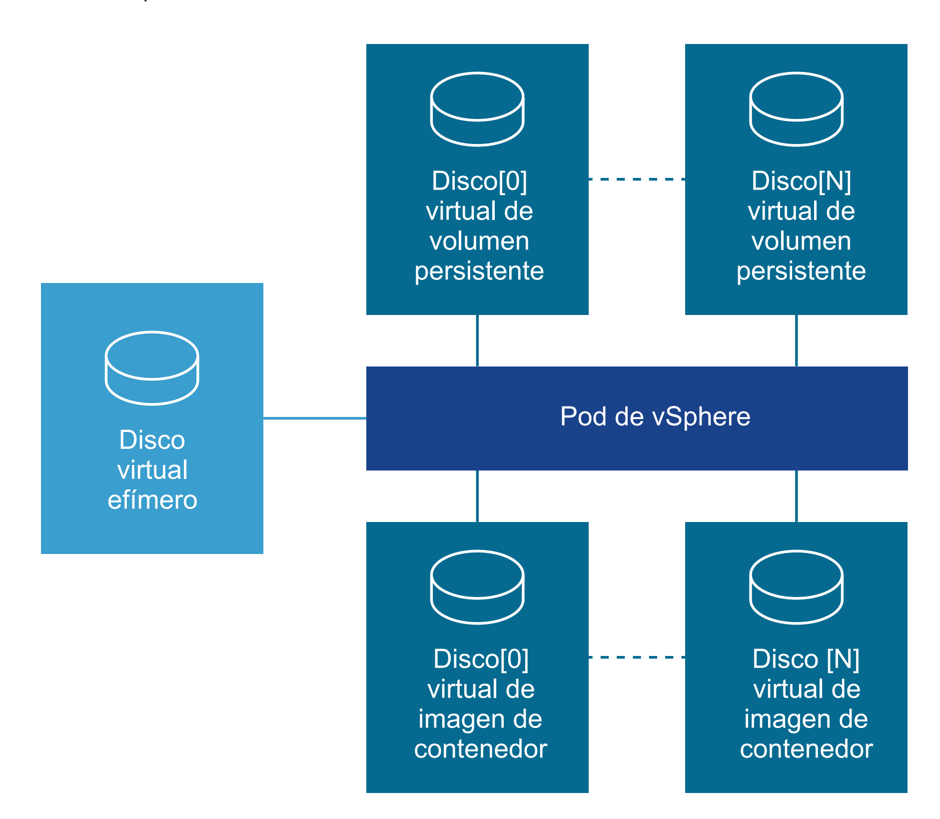
Almacenamiento de vSphere with Tanzu

vSphere with Tanzu utiliza directivas de almacenamiento para integrarse con almacenes de datos compartidos disponibles en el entorno, incluidos almacenes de datos de VMFS, NFS, vSAN o vVols. Las directivas representan los almacenes de datos y administran la colocación de almacenamiento de objetos, como las máquinas virtuales de plano de control, los discos efímeros del pod, las imágenes de contenedor y los volúmenes de almacenamiento persistente. Si utiliza clústeres de Tanzu Kubernetes, las directivas de almacenamiento también determinan cómo se implementan los nodos del clúster de Tanzu Kubernetes.

Antes de habilitar vSphere with Tanzu, cree las directivas de almacenamiento que clúster supervisor y los espacios de nombres usarán.

Según el entorno de almacenamiento de vSphere y las necesidades de desarrollo y operaciones, puede crear varias directivas de almacenamiento para representar diferentes clases de almacenamiento.

Por ejemplo, si un pod de vSphere monta todos los tres tipos de discos virtuales y su entorno de almacenamiento de vSphere tiene tres clases de almacenes de datos (Bronce, Plata y Oro), puede crear directivas de almacenamiento para todos los almacenes de datos. Posteriormente, puede utilizar el almacén de datos Bronce para los discos virtuales efímeros y los discos virtuales de imagen de contenedor, y utilizar los almacenes de datos Plata y Oro para los discos virtuales de volumen persistente.



Para obtener información general acerca de las directivas de almacenamiento, consulte el capítulo Administración basada en directiva de almacenamiento en la documentación de *Almacenamiento de vSphere*. Para obtener información sobre cómo crear directivas de almacenamiento, consulte Crear directivas de almacenamiento para vSphere with Tanzu.

Discos virtuales efímeros

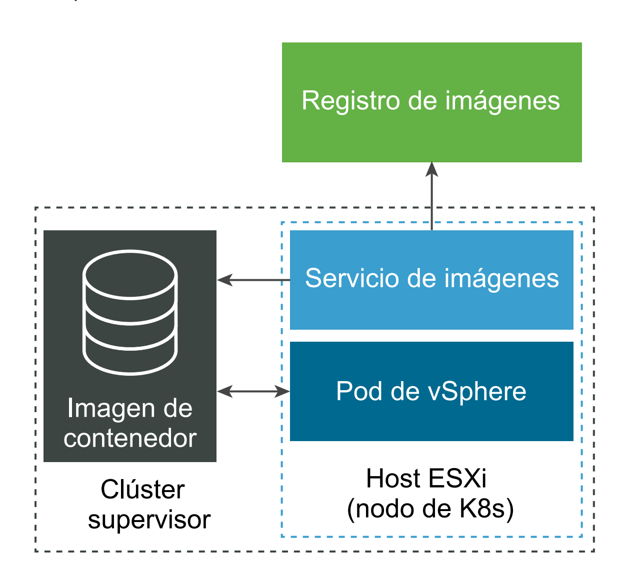
Un pod de vSphere y un pod que se ejecuta en un clúster de Tanzu Kubernetes requieren almacenamiento efímero para almacenar objetos de Kubernetes como registros, volúmenes `emptyDir` y `ConfigMaps` durante sus operaciones. Este almacenamiento efímero, o transitorio, dura mientras que el pod siga existiendo. Los datos efímeros se conservan entre los reinicios del contenedor, pero una vez que el pod llega al final de su vida, el disco virtual efímero desaparece.

Cada pod tiene un disco virtual efímero. Un administrador de vSphere utiliza una directiva de almacenamiento para definir la ubicación del almacén de datos de todos los discos virtuales efímeros al configurar el almacenamiento para el clúster supervisor.

Discos virtuales de imagen de contenedor

Los contenedores dentro del pod utilizan imágenes que incluyen el software que se ejecutará. El pod monta imágenes utilizadas por sus contenedores como discos virtuales de imagen. Cuando el pod completa su ciclo de vida, los discos virtuales de imagen se desasocian del pod.

El servicio de imágenes, un componente de ESXi, es responsable de extraer imágenes de contenedor del registro de imágenes y transformarlas en discos virtuales para ejecutarlas dentro del pod.



ESXi puede almacenar en la memoria caché las imágenes descargadas para los contenedores que se ejecutan en el pod. Los pods subsiguientes que utilizan la misma imagen la extraen de la memoria caché local en lugar del registro de contenedor externo.

Al igual que con los discos efímeros, el administrador de vSphere especifica la ubicación del almacén de datos para la memoria caché de imágenes a nivel del clúster supervisor. Consulte Capítulo 5 Configurar y administrar un clúster supervisor y Cambiar la configuración de almacenamiento en el clúster supervisor.

Para obtener información sobre cómo trabajar con las imágenes de contenedor, consulte Capítulo 15 Usar un registro de contenedores para cargas de trabajo de vSphere with Tanzu.

Discos virtuales de almacenamiento persistente

Ciertas cargas de trabajo de Kubernetes requieren almacenamiento persistente para almacenar datos de forma permanente. Para aprovisionar el almacenamiento persistente para cargas de trabajo de Kubernetes, la vSphere with Tanzu se integra con el almacenamiento nativo en la nube (Cloud Native Storage, CNS), un componente de vCenter Server que administra los volúmenes persistentes.

El almacenamiento persistente puede ser utilizado por pods de vSphere, clústeres de Tanzu Kubernetes y máquinas virtuales. Para que el almacenamiento persistente esté disponible para el equipo de Desarrollo y operaciones, los administradores de vSphere crean directivas de almacenamiento de máquina virtual que describen diferentes requisitos de almacenamiento y clases de servicios. A continuación, pueden asignar las directivas de almacenamiento a un espacio de nombres de vSphere. Consulte Creación y configuración de un espacio de nombres de vSphere y Cambiar la configuración de almacenamiento en un espacio de nombres.

Para obtener más información y detalles sobre cómo los clústeres de Tanzu Kubernetes y clúster supervisor usan el almacenamiento persistente, consulte Capítulo 10 Usar almacenamiento persistente en vSphere with Tanzu y Capítulo 13 Aprovisionar y operar clústeres TKGS.

Redes para vSphere with Tanzu

4

Un clúster supervisor puede utilizar la pila de redes de vSphere o VMware NSX-T™ Data Center para proporcionar conectividad a las máquinas virtuales, los servicios y las cargas de trabajo del plano de control de Kubernetes. Las redes que se utilizan para los clústeres de Tanzu Kubernetes aprovisionadas por servicio Tanzu Kubernetes Grid son una combinación del tejido que se encuentra subyacente a la infraestructura de vSphere with Tanzu y el software de código abierto que proporciona las redes para los pods, los servicios y las entradas del clúster.

Este capítulo incluye los siguientes temas:

- Redes del clúster supervisor
- Redes de clústeres de servicio Tanzu Kubernetes Grid
- Configurar NSX-T Data Center para vSphere with Tanzu
- Configurar redes de vSphere y NSX Advanced Load Balancer para vSphere with Tanzu
- Configurar redes de vSphere y el equilibrador de carga de HAProxy para vSphere with Tanzu

Redes del clúster supervisor

En un entorno de vSphere with Tanzu, una instancia de clúster supervisor puede utilizar la pila de redes de vSphere o VMware NSX-T Data Center™ para proporcionar conectividad a las máquinas virtuales, los servicios y las cargas de trabajo del plano de control de Kubernetes. Cuando se configura una instancia de clúster supervisor con la pila de redes de vSphere, todos los hosts del clúster se conectan a un conmutador vSphere Distributed Switch que proporciona conectividad a las máquinas virtuales de plano de control y las cargas de trabajo de Kubernetes. Una instancia de clúster supervisor que utiliza la pila de redes de vSphere requiere un equilibrador de carga en la red de administración de vCenter Server que proporcione conectividad a los usuarios de Desarrollo y operaciones, y a los servicios externos. Una instancia de clúster supervisor configurada con VMware NSX-T Data Center™, utiliza las redes basadas en software de la solución, así como un equilibrador de carga de NSX Edge para proporcionar conectividad a los servicios externos y a los usuarios de desarrollo y operaciones.

Redes de clúster supervisor con NSX-T Data Center

VMware NSX-T Data Center™ proporciona conectividad de red a los objetos dentro de clúster supervisor y las redes externas. La conectividad con los hosts ESXi que componen el clúster se gestiona mediante las redes vSphere estándar.

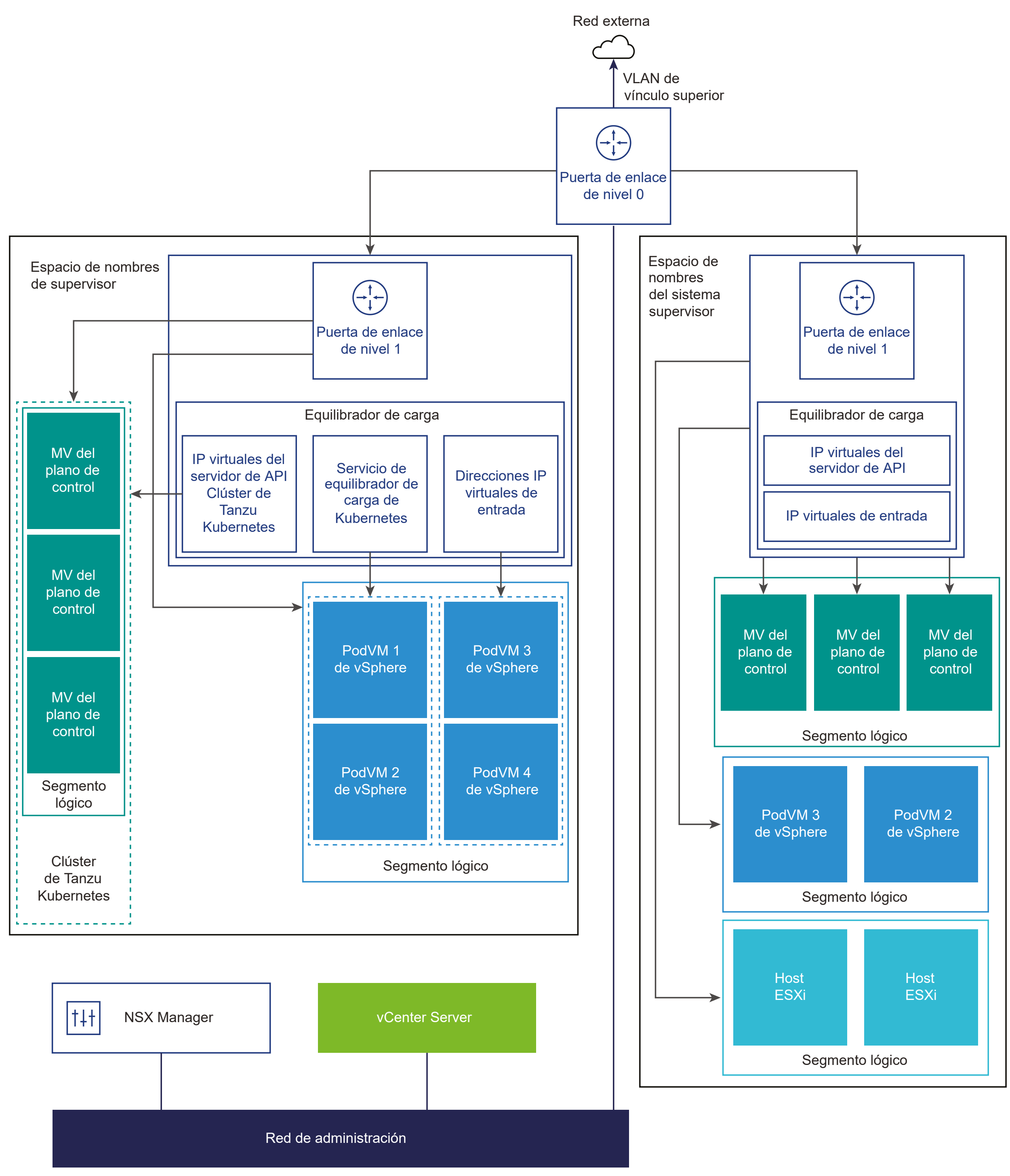
También puede configurar manualmente las redes de clúster supervisor mediante una implementación de NSX-T Data Center existente o mediante la implementación de una nueva instancia de NSX-T Data Center.

En la siguiente tabla se enumeran las versiones de NSX-T Data Center compatibles:

vSphere with Tanzu	NSX-T Data Center
Versión 7.0 Update 3	Versiones 3.0, 3.0.x, 3.1, 3.1.1, 3.1.2, y 3.1.3.
Versión 7.0 Update 2	Versiones 3.0, 3.0.x, 3.1, 3.1.1 y 3.1.2.
Versión 7.0 Update 1c	Versiones 3.0, 3.0.x, 3.1 y 3.1.1.
Versión 7.0 Update 1	Versiones 3.0, 3.0.1, 3.0.1.1 y 3.0.2.
Versión 7.0	Versión 3.0

En esta sección se describe la topología de red cuando se instala y configura la versión 7.0 Update 2 de vSphere with Tanzu. Para obtener información sobre la actualización cuando se actualiza de vSphere with Tanzu versión 7.0 Update 1 a la versión 7.0 Update 2, consulte Actualización de la topología de red .

Figura 4-1. Redes del clúster supervisor



- NSX Container Plug-in (NCP) proporciona integración entre NSX-T Data Center y Kubernetes. El componente principal de NCP se ejecuta en un contenedor y se comunica con NSX Manager y con el plano de control de Kubernetes. NCP supervisa los cambios en los contenedores y otros recursos, y administra los recursos de redes, como los puertos lógicos, los segmentos, los enrutadores y los grupos de seguridad de los contenedores mediante una llamada a NSX API.

NCP crea de forma predeterminada una puerta de enlace de nivel 1 compartida para los espacios de nombres del sistema y una puerta de enlace de nivel 1 y un equilibrador de carga para cada espacio de nombres. La puerta de enlace de nivel 1 está conectada a la puerta de enlace de nivel 0 y a un segmento predeterminado.

Los espacios de nombres del sistema son espacios de nombres que utilizan los componentes principales que son esenciales para el funcionamiento del clúster supervisor y Tanzu Kubernetes. Los recursos de red compartidos que incluyen la puerta de enlace de nivel 1, el equilibrador de carga y la IP de SNAT se agrupan en un espacio de nombres del sistema.

- NSX Edge proporciona conectividad de redes externas a objetos del clúster supervisor. El clúster de NSX Edge tiene un equilibrador de carga que proporciona redundancia a los servidores de API de Kubernetes que residen en las máquinas virtuales del plano de control, así como en cualquier aplicación que deba publicarse y a la que se pueda acceder desde fuera de clúster supervisor.
- Se asocia una puerta de enlace de nivel 0 al clúster de NSX Edge para proporcionar enrutamiento a la red externa. La interfaz de vínculo superior utiliza el protocolo de enrutamiento dinámico, BGP o enrutamiento estático.
- Cada espacio de nombres de vSphere tiene una red independiente y un conjunto de recursos de red compartidos por las aplicaciones que están dentro del espacio de nombres, como la puerta de enlace de nivel 1, el servicio de equilibrador de carga y la dirección IP de SNAT.
- Las cargas de trabajo que se ejecutan en pods de vSphere, máquinas virtuales normales o clústeres de Tanzu Kubernetes, los cuales están en el mismo espacio de nombres, comparten una misma IP de SNAT para la conectividad de norte a sur.
- Las cargas de trabajo que se ejecutan en pods de vSphere o en clústeres de Tanzu Kubernetes tendrán la misma regla de aislamiento que implementa el firewall predeterminado.
- No se requiere una IP de SNAT independiente para cada espacio de nombres de Kubernetes. La conectividad de este a oeste entre espacios de nombres no será SNAT.
- Los segmentos de cada espacio de nombres residen en la instancia de vSphere Distributed Switch (VDS) que funciona en el modo estándar y está asociada con el clúster de NSX Edge. El segmento proporciona una red de superposición al clúster supervisor.
- Los clústeres supervisores tienen segmentos separados dentro de la puerta de enlace de nivel 1 compartida. Para cada clúster de Tanzu Kubernetes, los segmentos se definen en la puerta de enlace de nivel 1 del espacio de nombres.
- Los procesos de Spherelet en cada host ESXi se comunican con vCenter Server a través de una interfaz de la red de administración.

Para obtener más información acerca de las redes de clúster supervisor, mire el video Servicio de red de vSphere 7 with Kubernetes, parte 1: el clúster supervisor.

Métodos de configuración de redes con NSX-T Data Center

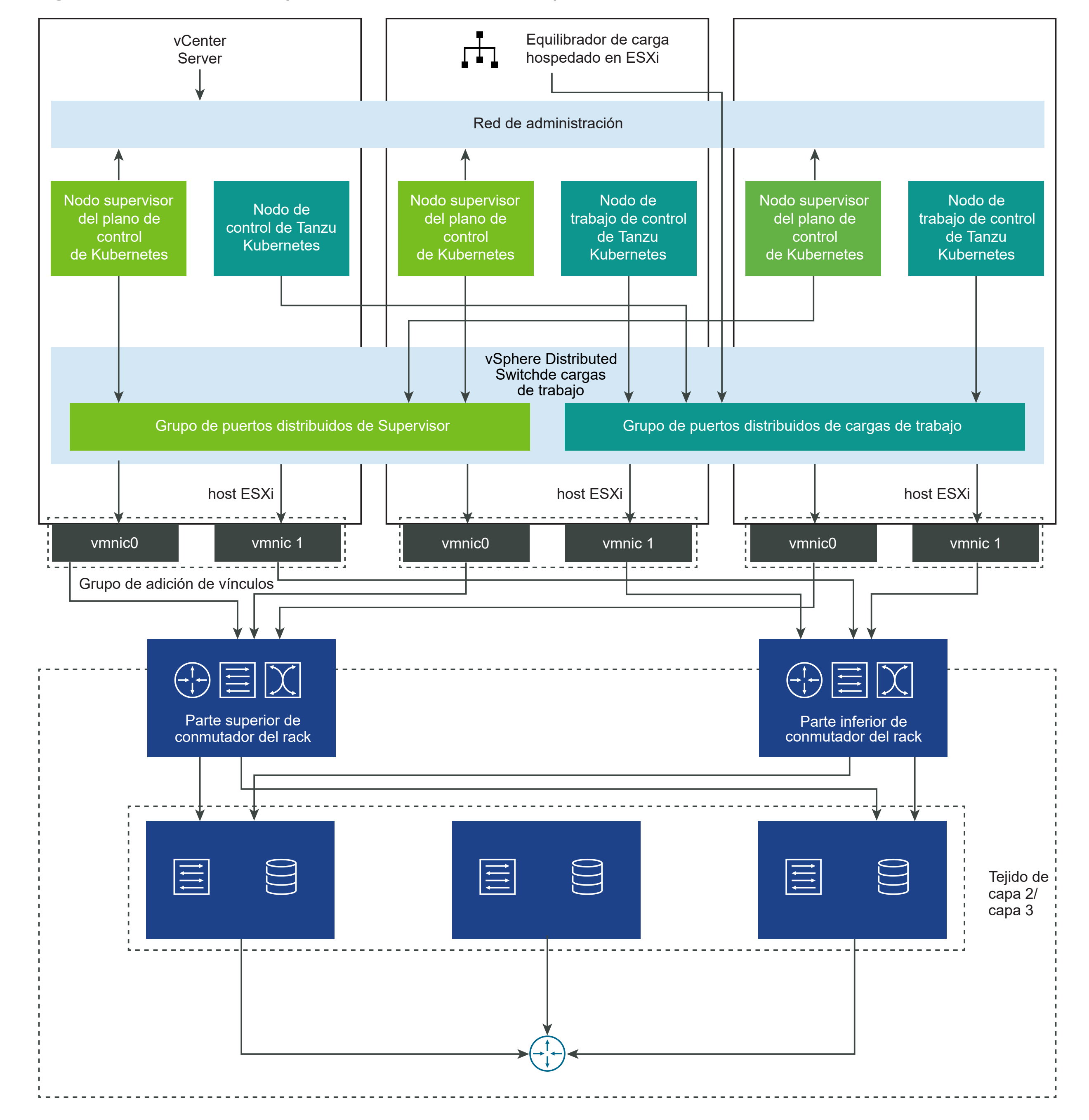
El clúster supervisor usa una configuración de redes taxativa. Existen dos métodos para configurar las redes de clúster supervisor con NSX-T Data Center que dan como resultado la implementación del mismo modelo de redes:

- La forma más sencilla de configurar las redes de clúster supervisor es mediante VMware Cloud Foundation SDDC Manager. Para obtener más información, consulte la documentación de VMware Cloud Foundation SDDC Manager. Para obtener más información, consulte Trabajar con la administración de cargas de trabajo.
- También puede configurar manualmente las redes de clúster supervisor mediante una implementación de NSX-T Data Center existente o mediante la implementación de una nueva instancia de NSX-T Data Center. Consulte Instalar y configurar NSX-T Data Center para vSphere with Tanzu para obtener más información.

Redes de clúster supervisor con vSphere Distributed Switch

Una instancia de clúster supervisor respaldada por un conmutador de vSphere Distributed Switch utiliza grupos de puertos distribuidos como redes de carga de trabajo para espacios de nombres.

Figura 4-2. Redes de espacio de nombres con vSphere Distributed Switch



En función de la topología que implemente para la instancia de clúster supervisor, puede usar uno o varios grupos de puertos distribuidos como redes de carga de trabajo. La red que proporciona conectividad a las máquinas virtuales del plano de control de Kubernetes se denomina "red de carga de trabajo principal". Puede asignar esta red a todos los espacios de nombres de la instancia de clúster supervisor o puede utilizar diferentes redes para cada espacio de nombres. Los clústeres de Tanzu Kubernetes se conectan a la red de carga de trabajo que se asigna al espacio de nombres en el que residen los clústeres.

Una instancia de clúster supervisor respaldada por un conmutador de vSphere Distributed Switch utiliza un equilibrador de carga para proporcionar conectividad a los usuarios de desarrollo y operaciones y los servicios externos. Puede utilizar el NSX Advanced Load Balancer o el equilibrador de carga de HAProxy.

Para obtener más información, consulte Configurar redes de vSphere y NSX Advanced Load Balancer para vSphere with Tanzu y Instalar y configurar el equilibrador de carga de HAProxy.

Redes de clústeres de servicio Tanzu Kubernetes Grid

Un clúster de servicio Tanzu Kubernetes Grid que lo aprovisiona servicio Tanzu Kubernetes Grid admite dos opciones de CNI: Antrea (opción predeterminada) y Calico. Ambas opciones son software de código abierto que proporcionan redes para pods, servicios e ingreso del clúster.

Los clústeres de servicio Tanzu Kubernetes Grid aprovisionados por el servicio Tanzu Kubernetes Grid admiten las siguientes opciones de interfaz de red de contenedor (Container Network Interface, CNI):

- Antrea
- Calico

Antrea es el CNI predeterminado para los nuevos clústeres de servicio Tanzu Kubernetes Grid. Si utiliza Antrea, no tiene que especificarlo como CNI durante el aprovisionamiento de los clústeres. Para utilizar Calico como el CNI, tiene dos opciones:

- Especifique el CNI directamente en el YAML del clúster. Consulte Ejemplos del aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1.
- Cambie el CNI predeterminado. Consulte Ejemplos de configuración de la API de servicio Tanzu Kubernetes Grid v1alpha1.

Nota El uso de Antrea como CNI predeterminado requiere una versión mínima del archivo OVA para los clústeres de servicio Tanzu Kubernetes Grid. Consulte Comprobar la compatibilidad del clúster de Tanzu Kubernetes para actualizar.

En la siguiente tabla se resumen las funciones de redes de los clústeres de servicio Tanzu Kubernetes Grid y su implementación.

Tabla 4-1. Redes de clústeres de servicio Tanzu Kubernetes Grid

Extremo	Proveedor	Descripción
Conectividad de pods	Antrea o Calico	Interfaz de red de contenedor para pods. Antrea utiliza Open vSwitch. Calico utiliza el puente de Linux con BGP.
Tipo de servicio: ClusterIP	Antrea o Calico	Tipo de servicio de Kubernetes predeterminado al que solo se puede acceder en el clúster.

Tabla 4-1. Redes de clústeres de servicio Tanzu Kubernetes Grid (continuación)

Extremo	Proveedor	Descripción
Tipo de servicio: NodePort	Antrea o Calico	Permite el acceso externo a través de un puerto abierto en cada nodo de trabajo mediante el proxy de red de Kubernetes.
Tipo de servicio: LoadBalancer	Equilibrador de carga de NSX-T, NSX Advanced Load Balancer, HAProxy	Para NSX-T, un servidor virtual por definición de tipo de servicio. Para NSX Advanced Load Balancer, consulte esa sección de esta documentación. **Nota** Es posible que algunas características de equilibrio de carga no estén disponibles con HAProxy, como la compatibilidad con IP estáticas.
Entrada de clúster	Controladora de entrada de terceros	Enrutamiento para el tráfico de pods de entrada; puede utilizar cualquier controladora de entrada de terceros, como Contour.
Directiva de red	Antrea o Calico	Controla el tráfico que se permite hacia y desde los pods seleccionados y los endpoints de red. Antrea utiliza Open vSwitch. Calico utiliza tablas de IP de Linux.

Configurar NSX-T Data Center para vSphere with Tanzu

vSphere with Tanzu requiere una configuración de redes específica para habilitar la conectividad con los clústeres supervisor y los espacios de nombres de vSphere, así como con todos los objetos que se ejecutan en los espacios de nombres, como los pods de vSphere, las máquinas virtuales y los clústeres de Tanzu Kubernetes. Como administrador de vSphere, instale y configure el NSX-T Data Center para vSphere with Tanzu.

El clúster supervisor usa una configuración de redes taxativa. Existen dos métodos para configurar las redes de clúster supervisor que dan como resultado la implementación del mismo modelo de redes:

- La forma más sencilla de configurar las redes de clúster supervisor es mediante VMware Cloud Foundation SDDC Manager. Para obtener más información, consulte la documentación de VMware Cloud Foundation SDDC Manager. Para obtener más información, consulte Trabajar con la administración de cargas de trabajo.
- También puede configurar manualmente las redes de clúster supervisor mediante una implementación de NSX-T Data Center existente o mediante la implementación de una nueva instancia de NSX-T Data Center.

clúster supervisor con el flujo de trabajo de NSX-T Data Center

Como administrador de vSphere, puede configurar un clúster de vSphere como un clúster supervisor con la pila de redes de vSphere.

Figura 4-3. clúster supervisor con el flujo de trabajo de redes de NSX-T Data Center

Procedimiento

1 Requisitos del sistema para configurar vSphere with Tanzu con NSX-T Data Center

Revise los requisitos del sistema para configurar vSphere with Tanzu en un clúster de vSphere mediante el uso de la pilas de redes de NSX-T Data Center.

2 Topologías de un clúster supervisor con NSX-T Data Center

Puede aplicar diferentes topologías al clúster dependiendo de las necesidades de sus cargas de trabajo de Kubernetes y de la infraestructura de redes subyacente.

3 Consideraciones sobre prácticas recomendadas para configurar el clúster supervisor con NSX-T Data Center

Tenga en cuenta estas prácticas recomendadas cuando configure un clúster de vSphere como un clúster supervisor con NSX-T Data Center.

4 Instalar y configurar NSX-T Data Center para vSphere with Tanzu

vSphere with Tanzu requiere una configuración de redes específica para habilitar la conectividad con los clústeres supervisor y los espacios de nombres de vSphere, así como con todos los objetos que se ejecutan en los espacios de nombres, como los pods de vSphere, las máquinas virtuales y los clústeres de Tanzu Kubernetes. Como administrador de vSphere, instale y configure el NSX-T Data Center para vSphere with Tanzu.

Requisitos del sistema para configurar vSphere with Tanzu con NSX-T Data Center

Revise los requisitos del sistema para configurar vSphere with Tanzu en un clúster de vSphere mediante el uso de la pilas de redes de NSX-T Data Center.

Límites de configuración de clústeres de vSphere with Tanzu

VMware proporciona límites de configuración en la herramienta Valores máximos de configuración de VMware.

Para los límites de configuración específicos de vSphere with Tanzu, incluidos los clústeres supervisor y los clústeres de Tanzu Kubernetes, seleccione **vSphere > vSphere 7.0 > vSphere with Kubernetes > VMware Tanzu Kubernetes Grid Service for vSphere** y haga clic en **Ver límites** o bien siga este vínculo.

Requisitos para un clúster de dominio de carga de trabajo, Edge y administración

vSphere with Tanzu se puede implementar con funciones de administración de cargas de trabajo, Edge y administración combinada en un único clúster de vSphere.

Tabla 4-2. Requisitos informáticos mínimos para el clúster de administración de cargas de trabajo, Edge y administración

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
vCenter Server 7.0	Pequeño	2	16 GB	290 GB
Hosts ESXi 7.0	3 hosts ESXi con 1 dirección IP estática por host. Si utiliza vSAN: 3 hosts ESXi con al menos 2 NIC físicas por host es el valor mínimo. Sin embargo, se recomienda utilizar 4 hosts ESXi por resistencia durante la aplicación de revisiones y la actualización. Los hosts deben unirse a un clúster con vSphere DRS y HA habilitados. vSphere DRS debe estar en el modo Totalmente automatizado o Parcialmente automatizado. **Precaución** No deshabilite vSphere DRS después de configurar el clúster supervisor. Tener DRS habilitado en todo momento es un requisito previo obligatorio para ejecutar cargas de trabajo en el clúster supervisor. Si se deshabilita DRS, se interrumpirán los clústeres de Tanzu Kubernetes.	8	64 GB por host	No aplicable
NSX Manager	Mediano	6	24 GB	300 GB
NSX Edge 1	Grande	8	32 GB	200 GB

Tabla 4-2. Requisitos informáticos mínimos para el clúster de administración de cargas de trabajo, Edge y administración (continuación)

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
NSX Edge 2	Grande	8	32 GB	200 GB
Máquinas virtuales de plano de control de Kubernetes	3	4	16 GB	16 GB

Topología con clúster de administración y Edge y clúster de administración de cargas de trabajo independientes

vSphere with Tanzu se puede implementar en dos clústeres, uno para las funciones de Edge y de administración, y otro dedicado a la administración de cargas de trabajo.

Tabla 4-3. Requisitos informáticos mínimos para el clúster de Edge y administración

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
vCenter Server 7.0	Pequeño	2	16 GB	290 GB
Hosts ESXi 7.0	2 hosts ESXi	8	64 GB por host	No aplicable
NSX Manager	Mediano	6	24 GB	300 GB
NSX Edge 1	Grande	8	32 GB	200 GB
NSX Edge 2	Grande	8	32 GB	200 GB

Tabla 4-4. Requisitos informáticos mínimos para el clúster de administración de cargas de trabajo

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
Hosts ESXi 7.0	3 hosts ESXi con 1 dirección IP estática por host. Si utiliza vSAN: 3 hosts ESXi con al menos 2 NIC físicas por host es el mínimo; sin embargo, se recomiendan 4 hosts ESXi para conseguir resiliencia durante la aplicación de revisiones y actualizaciones. Los hosts deben unirse a un clúster con vSphere DRS y HA habilitados. vSphere DRS debe estar en el modo Totalmente automatizado. **Precaución** No deshabilite vSphere DRS después de configurar el clúster supervisor. Tener DRS habilitado en todo momento es un requisito previo obligatorio para ejecutar cargas de trabajo en el clúster supervisor. Si se deshabilita DRS, se interrumpirán los clústeres de Tanzu Kubernetes.	8	64 GB por host	No aplicable
Máquinas virtuales de plano de control de Kubernetes	3	4	16 GB	16 GB

Requisitos de red

Independientemente de la topología que implemente para la administración de cargas de trabajo de Kubernetes en vSphere, la implementación debe cumplir los requisitos de red que se muestran en la siguiente tabla.

Nota No puede crear clústeres IPv6 con un clúster supervisor de vSphere 7 ni registrar clústeres IPv6 con Tanzu Mission Control.

Componente	Cantidad mínima	Configuración necesaria
IP estáticas para las máquinas virtuales del plano de control de Kubernetes	Bloque de 5	Un bloque de 5 direcciones IP estáticas consecutivas que se asignarán a las máquinas virtuales del plano de control de Kubernetes en el clúster supervisor.
Red de tráfico de administración	1	Una red de administración que se pueda enrutar a los hosts ESXi y a vCenter Server, y un servidor DHCP. La red debe poder acceder a un registro del contenedor y tener conectividad a Internet si el registro del contenedor se encuentra en la red externa. El registro del contenedor debe poder resolverse a través del DNS y la configuración de salida que se describe a continuación debe poder acceder a él.
Servidor NTP y DNS	1	Un servidor DNS y un servidor NTP que se pueden utilizar para vCenter Server. **Nota** Configure NTP en todos los hosts ESXi, los sistemas de vCenter Server y las instancias de NSX Manager.
servidor DHCP	1	Opcional. Configure un servidor DHCP para adquirir automáticamente direcciones IP para administración. El servidor DHCP debe admitir identificadores de cliente y proporcionar servidores DNS compatibles, dominios de búsqueda de DNS y un servidor NTP.
Registro de imágenes	1	Acceda a un registro para el servicio.

Componente	Cantidad mínima	Configuración necesaria
Subred de red de administración	1	La subred que se utiliza para el tráfico de administración entre los hosts ESXi y vCenter Server, las instancias de NSX Appliance y el plano de control de Kubernetes. El tamaño de la subred debe ser el siguiente: ■ Una dirección IP por adaptador de VMkernel de host. ■ Una dirección IP para vCenter Server Appliance. ■ Una o cuatro direcciones IP para NSX Manager. Cuatro cuando se realiza una agrupación de NSX Manager de 3 nodos y 1 IP virtual (VIP). ■ 5 direcciones IP para el plano de control de Kubernetes. 1 para cada uno de los 3 nodos, 1 para la IP virtual, 1 para la actualización sucesiva de clústeres. **Nota** La red de administración y la red de carga de trabajo deben estar en subredes diferentes. No se admite la asignación de la misma subred a las redes de administración y carga de trabajo, lo que puede provocar errores y problemas en el sistema.
VLAN de red de administración	1	Identificador de VLAN de la subred de la red de administración.

Componente	Cantidad mínima	Configuración necesaria
VLAN	3	Las IP de VLAN son las direcciones IP de los endpoints de túnel (Tunnel Endpoints, TEP). Los TEP del host ESXi y los TEP de Edge deben ser enrutables. Las direcciones IP de VLAN son necesarias para lo siguiente: ■ VTEP de host ESXi ■ VTEP de Edge con la IP estática ■ Puerta de enlace de nivel 0 y vínculo superior para el nodo de transporte. **Nota** El VTEP del host ESXi y el VTEP de Edge deben tener un tamaño de MTU superior a 1600. Los hosts ESXi y los nodos de NSX-T Edge actúan como endpoints de túnel y se asigna una IP de endpoint de túnel (Tunnel Endpoint, TEP) a cada nodo de Edge y host. Como las IP de TEP para hosts ESXi crean un túnel de superposición con IP de TEP en los nodos de Edge, las IP de VLAN deben poder enrutarse. Se requiere una VLAN adicional para proporcionar conectividad de norte a sur a la puerta de enlace de nivel 0. Los grupos de direcciones IP pueden compartirse entre clústeres. Sin embargo, el grupo de direcciones IP/VLAN de superposición de host no se debe compartir con la VLAN o el grupo de direcciones IP de superposición de Edge. **Nota** Si el TEP del host y el TEP de Edge usan diferentes NIC físicas, pueden utilizar la misma VLAN.
IP de vínculo superior de nivel 0	/24 direcciones IP privadas	La subred de IP que se utiliza para el vínculo superior de nivel 0. Los requisitos para la dirección IP del vínculo superior de nivel 0 son los siguientes: ■ 1 dirección IP, si no se requiere redundancia de Edge. ■ 4 direcciones IP; si utiliza BGP y redundancia de Edge, necesitará 2 direcciones IP por Edge. ■ 3 direcciones IP, si utiliza rutas estáticas y redundancia de Edge. La IP de administración de Edge, la subred, la puerta de enlace, la IP de vínculo superior, la subred y la puerta de enlace deben ser únicas.
MTU de red física	1.600	El tamaño de MTU debe ser 1600 o superior en cualquier red que transporte tráfico superpuesto.

Componente	Cantidad mínima	Configuración necesaria
Rango de CIDR del pod de vSphere	/23 direcciones IP privadas	Un rango de CIDR privado que proporciona direcciones IP a los pods de vSphere. Estas direcciones también se utilizan para los nodos del clúster de Tanzu Kubernetes. Debe especificar un rango de CIDR único del pod de vSphere para cada clúster. **Nota** El rango de CIDR del pod de vSphere y el rango de CIDR de las direcciones del servicio de Kubernetes no deben superponerse.
Rango de CIDR de servicios de Kubernetes	/16 direcciones IP privadas	Un rango de CIDR privado para asignar direcciones IP a los servicios de Kubernetes. Debe especificar un rango de CIDR único de servicios de Kubernetes para cada clúster supervisor.
Rango de CIDR de salida	/27 direcciones IP estáticas	Una anotación de CIDR privado para determinar la IP de egreso de los servicios de Kubernetes. Solo se asigna una dirección IP de egreso para cada espacio de nombres en el clúster supervisor. La IP de egreso es la dirección que las entidades externas utilizan para comunicarse con los servicios en el espacio de nombres. La cantidad de direcciones IP de egreso limita el número de directivas de egreso que puede tener el clúster supervisor. El valor mínimo es un CIDR de /27 o más. Por ejemplo, `10.174.4.96/27` **Nota** Las direcciones IP de egreso y las direcciones IP de entrada no deben superponerse.
CIDR de entrada	/27 direcciones IP estáticas	Un rango de CIDR privado que se utilizará para las direcciones IP de entradas. La entrada permite aplicar directivas de tráfico a las solicitudes que entran en clúster supervisor desde redes externas. La cantidad de direcciones IP de entrada limita el número de entradas que puede tener el clúster. El valor mínimo es un CIDR de /27 o más. **Nota** Las direcciones IP de egreso y las direcciones IP de entrada no deben superponerse.

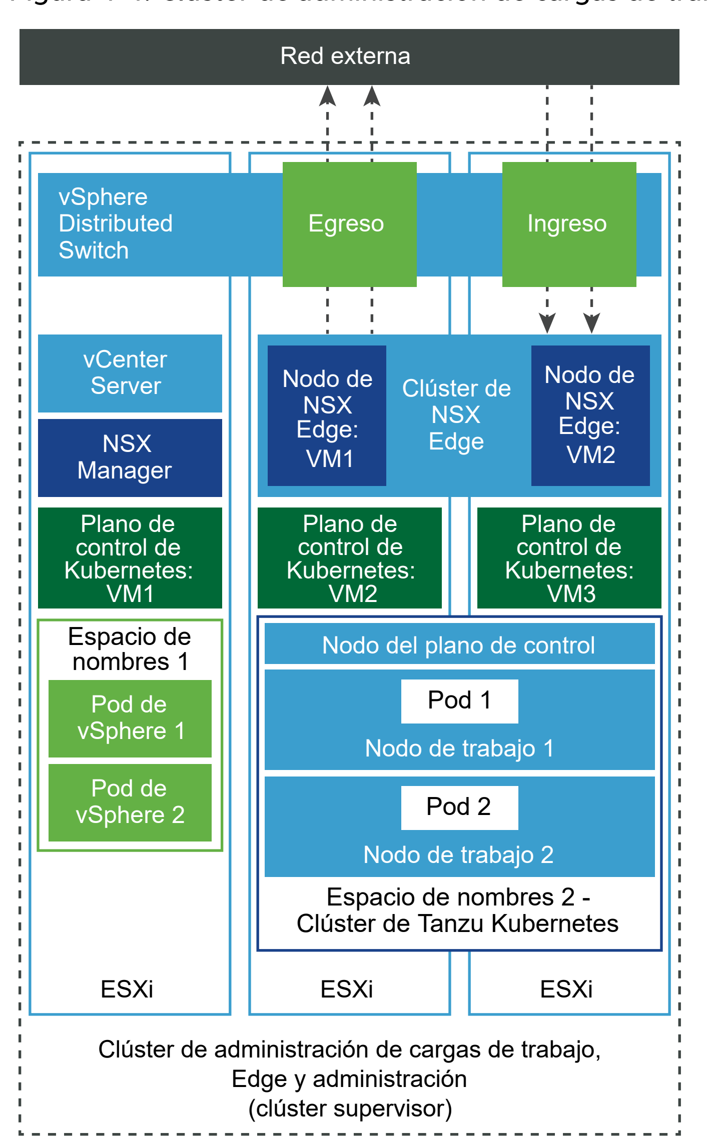
Topologías de un clúster supervisor con NSX-T Data Center

Puede aplicar diferentes topologías al clúster dependiendo de las necesidades de sus cargas de trabajo de Kubernetes y de la infraestructura de redes subyacente.

Topología para un clúster de dominio de carga de trabajo, Edge y administración

vSphere with Tanzu se puede implementar con funciones de administración de cargas de trabajo, Edge y administración combinada en un único clúster de vSphere.

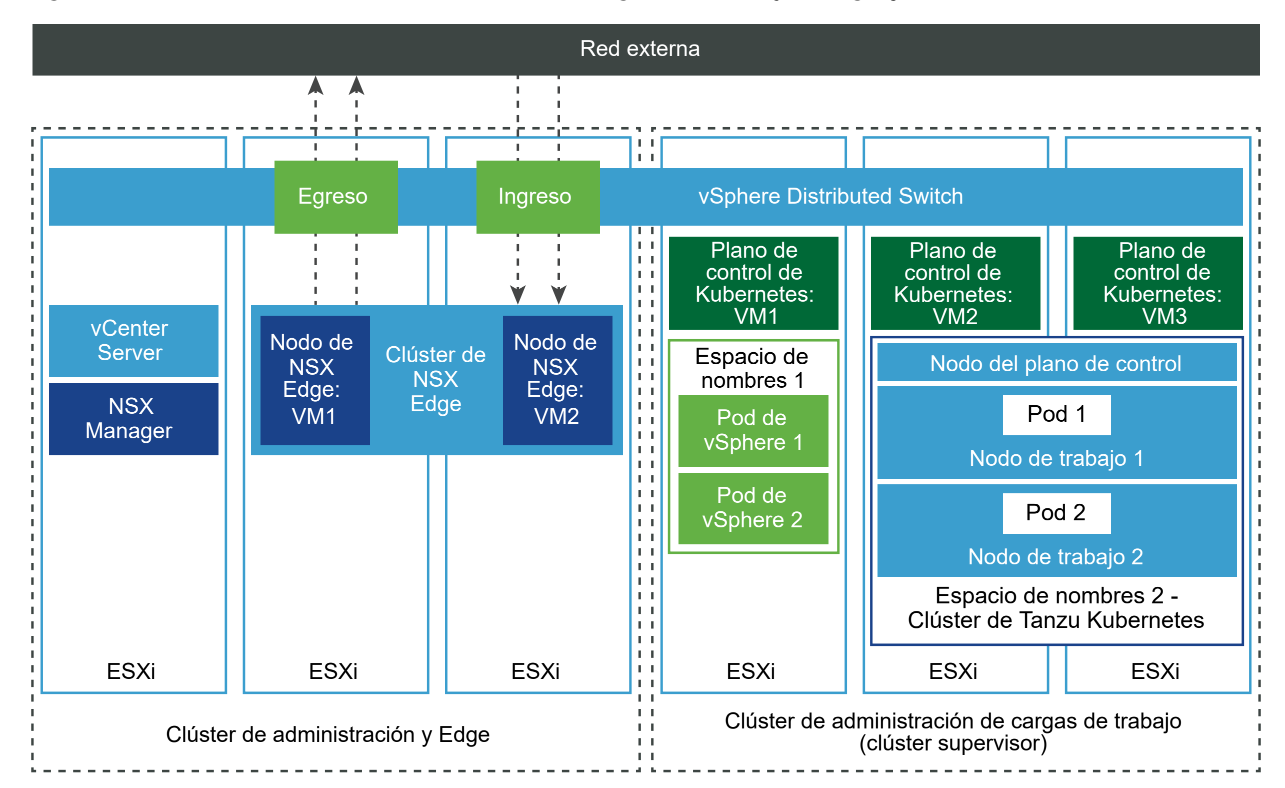
Figura 4-4. Clúster de administración de cargas de trabajo, Edge y administración



Topología con clúster de administración y Edge y clúster de administración de cargas de trabajo independientes

vSphere with Tanzu se puede implementar en dos clústeres, uno para las funciones de Edge y de administración, y otro dedicado a la administración de cargas de trabajo.

Figura 4-5. Clústeres de administración de cargas de trabajo, Edge y administración



Consideraciones sobre prácticas recomendadas para configurar el clúster supervisor con NSX-T Data Center

Tenga en cuenta estas prácticas recomendadas cuando configure un clúster de vSphere como un clúster supervisor con NSX-T Data Center.

- Utilice un almacén de datos de vSAN para las instancias de NSX Edge.
- Si usa un almacén de datos de vSAN, asegúrese de que el entorno de vSAN tenga el tamaño adecuado para las cargas de trabajo. La configuración de vSAN requiere más memoria, ya que se utiliza la memoria del kernel para vSAN. Esto reduce la memoria disponible para las máquinas virtuales de NSX Edge. Utilice la calculadora de vSAN para obtener el tamaño correcto. Para obtener más información, consulte vSAN ReadyNode Sizer.
- Si utiliza un almacén de datos de NFS, compruebe que se comparte entre todos los hosts del clúster. Cree un almacén de datos NFS único para cada nodo de NSX Edge.
- Configure un grupo de recursos dedicado para cada clúster de NSX Edge. No comparta el grupo de recursos con otras máquinas virtuales.
- Cuando configure la superposición de hosts ESXi, use VLAN dentro del rango de 1 a 4094.
- Cuando configure la superposición de instancias de Edge, use VLAN dentro del rango de 1 a 4094.

Instalar y configurar NSX-T Data Center para vSphere with Tanzu

vSphere with Tanzu requiere una configuración de redes específica para habilitar la conectividad con los clústeres supervisor y los espacios de nombres de vSphere, así como con todos los objetos que se ejecutan en los espacios de nombres, como los pods de vSphere, las máquinas virtuales y los clústeres de Tanzu Kubernetes. Como administrador de vSphere, instale y configure el NSX-T Data Center para vSphere with Tanzu.

En esta sección se describe cómo configurar las redes de clúster supervisor mediante la implementación de una nueva instancia de NSX-T Data Center, pero los procedimientos se aplican también a una implementación de NSX-T Data Center existente. En esta sección también se proporciona información general para comprender cómo actúa VMware Cloud Foundation SDDC Manager cuando configura el dominio de carga de trabajo de clúster supervisor.

Requisitos previos

- Compruebe que el entorno cumpla con los requisitos del sistema para configurar un clúster de vSphere como un clúster supervisor. Para obtener información sobre los requisitos, consulte Requisitos del sistema para configurar vSphere with Tanzu con NSX-T Data Center.
- Asigne la licencia de VMware vSphere 7 Enterprise Plus with Add-on for Kubernetes a todos los hosts ESXi que formarán parte de clúster supervisor.
- Cree directivas de almacenamiento para la colocación de las máquinas virtuales del plano de control, los discos efímeros del pod y las imágenes del contenedor.
- Configure el almacenamiento compartido para el clúster. Se requiere almacenamiento compartido para vSphere DRS, HA y el almacenamiento de volúmenes persistentes de contenedores.
- Compruebe que DRS y HA estén habilitados en el clúster de vSphere y que DRS esté en el modo totalmente automatizado.
- Compruebe que tenga el privilegio **Modificar configuración de todo el clúster** en el clúster.

Crear vSphere Distributed Switch

Para controlar la configuración de redes de todos los hosts de clúster supervisor, cree una instancia de vSphere Distributed Switch.

Procedimiento

1 En vSphere Client, desplácese hasta un centro de datos.

2 En el navegador, haga clic con el botón derecho en el centro de datos y seleccione **Conmutador distribuido > Nuevo conmutador distribuido**.

3 Introduzca un nombre para el nuevo conmutador distribuido.

   Por ejemplo, `DSwitch`.

4 En **Seleccionar versión**, introduzca una versión para el conmutador distribuido.

   Seleccione **7.0.0 - ESXi 7.0 y versiones posteriores**.

5 En **Configurar parámetros**, introduzca la cantidad de puertos de vínculo superior.

   Introduzca un valor de `2`.

6 Revise la configuración y haga clic en **Finalizar**.

7 Haga clic con el botón derecho en el conmutador distribuido que ha creado y seleccione **Configuración > Editar configuración**.

8 En la pestaña **Avanzado**, introduzca un valor superior a 1600 como valor de MTU (bytes) y haga clic en **Aceptar**.

   El tamaño de MTU debe ser 1600 o superior en cualquier red que transporte tráfico superpuesto.

   Por ejemplo, `9000`.

Pasos siguientes

Agregue grupos de puertos distribuidos. Consulte Crear grupos de puertos distribuidos.

Crear grupos de puertos distribuidos

Cree grupos de puertos distribuidos para cada vínculo superior del nodo de NSX Edge, TEP de nodo de Edge, red de administración y almacenamiento compartido.

Requisitos previos

Compruebe que se haya creado una instancia de vSphere Distributed Switch.

Procedimiento

1 En vSphere Client, desplácese hasta un centro de datos.

2 En el navegador, haga clic con el botón derecho en el conmutador distribuido y seleccione **Grupo de puertos distribuidos > Nuevo grupo de puertos distribuidos**.

3 Cree un grupo de puertos para el vínculo superior de NSX Edge.

   Por ejemplo, `DPortGroup-EDGE-UPLINK`.

4 Configure **Tipo de VLAN** como enlace troncal de VLAN.

5 Haga clic con el botón derecho en el conmutador distribuido y en el menú **Acciones**, seleccione **Grupo de puertos distribuidos > Administrar grupo de puertos distribuidos**.

6 Seleccione **Formación de equipos y conmutación por error** y haga clic en **Siguiente**.

7 Configure vínculos superiores activos y en espera.

   Por ejemplo, el vínculo superior es `Uplink1` y el vínculo superior en espera es `Uplink2`.

8 Repita los pasos 4 a 7 para el TEP del nodo de Edge, la red de administración y el almacenamiento compartido.

   Por ejemplo, cree los siguientes grupos de puertos:

Grupo de puertos	Nombre	tipo de VLAN
TEP de nodo de Edge	`DPortGroup-EDGE-TEP`	Configure **Tipo de VLAN** como enlace troncal de VLAN. Configure el vínculo superior activo como `Uplink2` y el vínculo superior en espera como `Uplink1`. **Nota** La VLAN que se utiliza para el TEP de nodos de Edge debe ser diferente de la VLAN utilizada para el TEP de ESXi.
Administración	`DPortGroup-MGMT`	Configure **Tipo de VLAN** como VLAN e introduzca el identificador de VLAN de la red de administración. Por ejemplo, `1060`.
Almacenamiento compartido o vSAN	`DPortGroup-VSAN`	Configure **Tipo de VLAN** como VLAN e introduzca el identificador de VLAN. Por ejemplo, `3082`.

9 (opcional) Cree grupos de puertos para los siguientes componentes:

- vSphere vMotion
- Tráfico de máquina virtual

Pasos siguientes

Agregue hosts a la instancia de vSphere Distributed Switch. Consulte Agregar hosts a la instancia de vSphere Distributed Switch.

Agregar hosts a la instancia de vSphere Distributed Switch

Para administrar las redes de su entorno mediante vSphere Distributed Switch, debe asociar los hosts con el conmutador. Para ello, conecte las NIC físicas, los adaptadores de VMkernel y los adaptadores de red de las máquinas virtuales de los hosts al conmutador distribuido.

Requisitos previos

- Compruebe que haya suficientes vínculos superiores disponibles en el conmutador distribuido para asignarles las NIC físicas que desea conectar al conmutador.
- Compruebe que haya al menos un grupo de puertos distribuidos disponible en el conmutador distribuido.
- Compruebe que el grupo de puertos distribuidos tenga configurados vínculos superiores activos en su directiva de formación de equipos y conmutación por error.

Procedimiento

1 En vSphere Client, seleccione **Redes** y desplácese al conmutador distribuido.

2 En el menú **Acciones**, seleccione **Agregar y administrar hosts**.

3 En la página **Seleccionar tarea**, seleccione **Agregar hosts** y haga clic en **Siguiente**.

4 En la página **Seleccionar hosts**, haga clic en **Nuevos hosts**, seleccione los hosts del centro de datos, haga clic en **Aceptar** y, a continuación, haga clic en **Siguiente**.

5 En la página **Administrar adaptadores físicos**, configure las NIC físicas en el conmutador distribuido.

   a En la lista **En otros conmutadores/sin reclamar**, seleccione una NIC física.

      Si selecciona NIC físicas que ya están conectadas a otros conmutadores, estas se migrarán al conmutador distribuido actual.

   b Haga clic en **Asignar vínculo superior**.

   c Seleccione un vínculo superior.

   d Para asignar el vínculo superior a todos los hosts del clúster, seleccione **Aplicar esta asignación de vínculo superior al resto de los hosts**.

   e Haga clic en **Aceptar**.

   Por ejemplo, asigne `Uplink 1` a `vmnic0` y `Uplink 2` a `vmnic1`.

6 Haga clic en **Siguiente**.

7 En la página **Administrar adaptadores de VMkernel**, configure los adaptadores de VMkernel.

   a Seleccione un adaptador VMkernel y haga clic en **Asignar grupo de puertos**.

   b Seleccione un grupo de puertos distribuidos.

      Por ejemplo, **DPortGroup**.

   c Para aplicar el grupo de puertos a todos los hosts del clúster, seleccione **Aplicar esta asignación de grupo de puertos al resto de los hosts**.

   d Haga clic en **Aceptar**.

8 Haga clic en **Siguiente**.

9 (opcional) En la página **Migrar redes de máquina virtual**, active la casilla **Migrar redes de máquinas virtuales** para configurar las redes de máquinas virtuales.

   a Para conectar todos los adaptadores de red de una máquina virtual a un grupo de puertos distribuido, seleccione la máquina virtual o seleccione un adaptador de red individual para conectar solamente el adaptador.

   b Haga clic en **Asignar grupo de puertos**.

   c Seleccione un grupo de puertos distribuidos de la lista y haga clic en **Aceptar**.

   d Haga clic en **Siguiente**.

Pasos siguientes

Implemente y configure el NSX Manager. Consulte Implementar y configurar el NSX Manager

Implementar y configurar el NSX Manager

Puede usar la instancia de vSphere Client para implementar NSX Manager en el clúster de vSphere y utilizarlo con vSphere with Tanzu.

Para implementar la instancia de NSX Manager con el archivo OVA, realice los pasos de este procedimiento.

Para obtener información sobre la implementación de NSX Manager a través de la interfaz de usuario o la CLI, consulte la *Guía de instalación de NSX-T Data Center*.

Requisitos previos

- Compruebe que el entorno cumpla con los requisitos de red. Consulte Requisitos del sistema para configurar vSphere with Tanzu con NSX-T Data Center para obtener más detalles.
- Compruebe que los puertos necesarios estén abiertos. Para obtener información sobre los puertos y los protocolos, consulte la *Guía de instalación de NSX-T Data Center*.

Procedimiento

1. Busque el archivo OVA de NSX-T Data Center en el portal de descargas de VMware.

   Copie la URL de descarga o descargue el archivo OVA.
2. Haga clic con el botón secundario del ratón y seleccione **Implementar plantilla de OVF** para iniciar el Asistente de instalación.
3. En la pestaña **Seleccione una plantilla de archivo OVF**, introduzca la URL de descarga de OVA o desplácese hasta el archivo OVA.
4. En la pestaña **Seleccionar un nombre y una carpeta**, escriba un nombre para la máquina virtual de NSX Manager.
5. En la pestaña **Seleccionar un recurso informático**, seleccione el clúster de vSphere en el que se implementará NSX Manager.
6. Haga clic en **Siguiente** para revisar los detalles.
7. En la pestaña **Configuración**, seleccione el tamaño de implementación de NSX-T.

   El tamaño de implementación mínimo recomendado es Medio.
8. En la pestaña **Seleccionar almacenamiento**, seleccione el almacenamiento compartido para la implementación.
9. Para habilitar el aprovisionamiento fino, seleccione **Aprovisionamiento fino** en **Seleccionar formato de disco virtual**.

   Los discos virtuales cuentan con aprovisionamiento grueso de forma predeterminada.
10. En la pestaña **Seleccionar redes**, seleccione el grupo de puertos de administración o la red de destino para NSX Manager en **Red de destino**.

    Por ejemplo, `DPortGroup-MGMT`.

11 En la pestaña **Personalizar plantilla**, introduzca la raíz del sistema, el administrador de la CLI y las contraseñas de auditoría de NSX Manager. Las contraseñas deben cumplir con las restricciones de seguridad para contraseñas.

   - Al menos 12 caracteres.
   - Al menos una letra en minúsculas.
   - Al menos una letra en mayúsculas.
   - Al menos un dígito.
   - Al menos un carácter especial.
   - Al menos cinco caracteres diferentes.
   - El módulo PAM de Linux aplica las reglas de complejidad de contraseña predeterminadas.

12 Introduzca la puerta de enlace IPv4 predeterminada, la red de administración IPv4, la máscara de red de la red de administración, el servidor DNS, la lista de búsqueda de dominios y la dirección IP de NTP.

13 Habilite SSH y permita el inicio de sesión SSH raíz en la línea de comandos de NSX Manager.

   De forma predeterminada, las opciones SSH están deshabilitadas por motivos de seguridad.

14 Compruebe que la especificación de la plantilla de OVF personalizada sea correcta y haga clic en **Finalizar** para iniciar la instalación.

15 Después de que arranque NSX Manager, inicie sesión en la CLI como administrador y ejecute el comando `get interface eth0` para comprobar que la dirección IP se aplicó según lo previsto.

16 Introduzca el comando `get services` para comprobar que se están ejecutando todos los servicios.

Implementar nodos de NSX Manager para formar un clúster

Un clúster de NSX Manager proporciona alta disponibilidad. Los nodos de NSX Manager solo se pueden implementar mediante la interfaz de usuario en los hosts ESXi que administra vCenter Server. Para crear un clúster de NSX Manager, implemente dos nodos adicionales con la finalidad de formar un clúster de tres nodos en total. Cuando se implementa un nodo nuevo desde la interfaz de usuario, este se conecta al primer nodo implementado para formar un clúster. Todos los detalles del repositorio y la contraseña del primer nodo implementado se sincronizan con el nodo que se acaba de implementar.

Requisitos previos

- Compruebe que se haya instalado un nodo de NSX Manager.
- Compruebe que se haya configurado un administrador de equipo.
- Compruebe que los puertos necesarios estén abiertos.
- Compruebe que se haya configurado un almacén de datos en el host ESXi.

- Compruebe que tenga la dirección IP y la puerta de enlace, las direcciones IP del servidor DNS, la lista de búsqueda de dominios y la dirección IP del servidor NTP que utilizará NSX Manager.
- Compruebe que tenga una red de grupos de puertos de máquina virtual de destino. Coloque los dispositivos de NSX-T Data Center en una red de máquinas virtuales de administración.

Procedimiento

1 Desde un explorador, inicie sesión con privilegios de administrador en NSX Manager en https://<manager-ip-address>.

2 Para implementar un dispositivo, seleccione **Sistema > Dispositivos > Agregar NSX Appliance**.

3 Introduzca los detalles del dispositivo.

Opción	Descripción
Nombre de host	Introduzca el nombre del host o el FQDN que se utilizará para el nodo.
Dirección IP/máscara de red de administración	Introduzca una dirección IP que se asignará al nodo.
Puerta de enlace de administración	Introduzca una dirección IP de puerta de enlace que vaya a utilizar el nodo.
Servidores DNS	Introduzca la lista de direcciones IP del servidor DNS que vaya a utilizar el nodo.
Servidor NTP	Introduzca la lista de direcciones IP del servidor NTP.
Tamaño del nodo	Seleccione el formato **Mediano (6 vCPU, 24 GB de RAM, 300 GB de almacenamiento)** en las opciones.

4 Introduzca los detalles de configuración del dispositivo.

Opción	Descripción
Administrador de equipo	Seleccione la instancia de vCenter Server que configuró como administrador de equipo.
Clúster de proceso	Seleccione el clúster al que se debe unir el nodo.
Almacén de datos	Seleccione un almacén de datos para los archivos de nodo.
Formato de disco virtual	Seleccione el formato **Aprovisionamiento fino**.
Red	Haga clic en **Seleccionar red** para seleccionar la red de administración del nodo.

5 Introduzca los detalles de acceso y las credenciales.

Opción	Descripción
Habilitar SSH	Active el botón para permitir el inicio de sesión SSH en el nodo nuevo.
Habilitar el acceso raíz	Active el botón para permitir el acceso raíz en el nodo nuevo.

Opción	Descripción
Credenciales raíz del sistema	Establezca la contraseña raíz y confírmela para el nodo nuevo. La contraseña debe cumplir las restricciones de seguridad para contraseñas. ■ Al menos 12 caracteres. ■ Al menos una letra en minúsculas. ■ Al menos una letra en mayúsculas. ■ Al menos un dígito. ■ Al menos un carácter especial. ■ Al menos cinco caracteres diferentes. ■ El módulo PAM de Linux aplica las reglas de complejidad de contraseña predeterminadas.
Credenciales de la CLI de administración y credenciales de la CLI de auditoría	Seleccione la casilla de verificación **Igual que la contraseña raíz** si desea usar la misma contraseña que configuró para la raíz; de lo contrario, anule la selección de esta casilla y establezca otra contraseña diferente.

6 Haga clic en **Instalar dispositivo**.

   Se implementará el nodo nuevo. Puede realizar un seguimiento del proceso de implementación en la página **Sistema> > Dispositivos**. No agregue más nodos hasta que finalice la instalación y el clúster esté estable.

7 Espere a que finalice la implementación, la creación del clúster y la sincronización del repositorio.

   El proceso de unión y estabilización del clúster puede tardar entre 10 y 15 minutos. Compruebe que el estado de cada grupo de servicios del clúster sea `ACTIVO` antes de realizar cualquier otro cambio en el clúster.

8 Después de que arranque el nodo, inicie sesión en la CLI como administrador y ejecute el comando `get interface eth0` para comprobar que la dirección IP se aplicó según lo previsto.

9 Si el clúster solo tiene dos nodos, agregue otro dispositivo. Seleccione **Sistema > Dispositivos > Agregar NSX Appliance** y repita los pasos de configuración.

Agregar una licencia

Agregue una licencia mediante el NSX Manager.

Requisitos previos

Obtenga una licencia Avanzada o superior de NSX-T Data Center.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Licencias > Agregar**.

3 Introduzca la clave de licencia.

4 Haga clic en **Agregar**.

Agregar un administrador de equipo

Un administrador de equipo es una aplicación que gestiona recursos como hosts y máquinas virtuales. Configure la instancia de vCenter Server que está asociada con la instancia de NSX-T Data Center como administrador de equipo en NSX Manager.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Administradores de equipo > Agregar**

3 Introduzca los detalles del administrador de equipo.

Opción	Descripción
Nombre y descripción	Introduzca el nombre y la descripción del vCenter Server.
FQDN o dirección IP	Introduzca el FQDN o la dirección IP de la instancia del vCenter Server.
Nombre de usuario y contraseña	Introduzca las credenciales de inicio de sesión de vCenter Server.

4 Seleccione **Habilitar confianza** para permitir que vCenter Server se comunique con NSX-T Data Center.

5 Si no proporcionó un valor de huella digital para NSX Manager, el sistema identificará la huella digital y la mostrará.

6 Haga clic en **Agregar** para aceptar la huella digital.

Resultados

Después de cierto tiempo, el administrador de equipos se registra en vCenter Server y el estado de la conexión cambia a `Activo`. Si el FQDN o el PNID de vCenter Server cambian, debe volver a registrarlos en NSX Manager. Para obtener más información, consulte Registrar vCenter Server en NSX Manager.

Nota Después de que el vCenter Server se registre correctamente, no apague ni elimine la máquina virtual de NSX Manager sin eliminar primero el administrador de equipo. De lo contrario, cuando implemente un nuevo NSX Manager, no podrá volver a registrar el mismo vCenter Server. Recibirá un error que indica que vCenter Server ya se registró en otra instancia de NSX Manager.

Puede hacer clic en el nombre del administrador de equipo para ver los detalles, editar el administrador de equipo o administrar las etiquetas que se aplican al administrador de equipo.

Crear zonas de transporte

Las zonas de transporte indican los hosts y las máquinas virtuales que pueden utilizar una red determinada. Una zona de transporte puede abarcar uno o varios clústeres de host.

Como administrador de vSphere, utilice las zonas de transporte predeterminadas o cree las siguientes:

- Una zona de transporte superpuesta que utilizan las máquinas virtuales del plano de control del clúster supervisor.
- Una zona de transporte de VLAN para los nodos de NSX Edge que se utilizará para los vínculos superiores a la red física.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Zonas de transporte > Agregar**.

3 Introduzca un nombre para la zona de transporte y, opcionalmente, una descripción.

4 Seleccione un tipo de tráfico.

   Puede seleccionar **Superposición** o **VLAN**.

   Las siguientes zonas de transporte existen de forma predeterminada:

   - Una zona de transporte de VLAN con el nombre `nsx-vlan-transportzone`.
   - Una zona de transporte superpuesta con el nombre `nsx-overlay-transportzone`.

5 (opcional) Introduzca uno o varios nombres de directiva de formación de equipos de enlace ascendente.

   Los segmentos asociados a las zonas de transporte usan estas directivas de formación de equipos con nombre. Si los segmentos no encuentran una directiva de formación de equipos con nombre que coincida, se utilizará la directiva de formación de equipos de vínculo superior predeterminada.

Resultados

La nueva zona de transporte aparece en la página **Zonas de transporte**.

Crear un grupo de direcciones IP para las direcciones IP del endpoint de túnel del host

Cree grupos de direcciones IP para los endpoints de túnel del host ESXi (TEP) y los nodos de Edge. Los TEP son las direcciones IP de origen y destino que se utilizan en el encabezado IP externo para identificar los hosts ESXi que originan y finalizan la encapsulación NSX-T de tramas superpuestas. Puede utilizar DHCP o grupos de direcciones IP configuradas manualmente para las direcciones IP de TEP.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Redes > Grupos de direcciones IP > Agregar grupo de direcciones IP**.

3 Introduzca los siguientes detalles del grupo de direcciones IP.

Opción	Descripción
Nombre y descripción	Introduzca el nombre del grupo de direcciones IP y la descripción opcional. Por ejemplo, `ESXI-TEP-IP-POOL`.
Rangos de IP	Introduzca el rango de asignación de IP. Por ejemplo, `10.197.79.158 - 10.197.79.160`
Puerta de enlace	Introduzca la dirección IP de la puerta de enlace. Por ejemplo, `10.197.79.253`.
CIDR	Introduzca la dirección de red en una notación CIDR. Por ejemplo, `10.197.79.0/24`.

4 Haga clic en **Agregar** y **Aplicar**.

5 Repita los pasos 2 a 4 para crear un grupo de direcciones IP para los nodos de Edge.

Por ejemplo, `EDGE-TEP-IP-POOL`.

6 Compruebe que los grupos de direcciones IP de TEP que creó aparezcan en la página **Grupo de direcciones IP**.

Crear un perfil de host de vínculo superior

Un perfil de host de vínculo superior define las directivas para los vínculos superiores de los hosts ESXi a los segmentos de NSX-T Data Center.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Perfiles > Perfiles de vínculo superior > Agregar**.

3 Introduzca un nombre para el perfil de vínculo superior y, si lo desea, una descripción del perfil de vínculo superior.

Por ejemplo, `ESXI-UPLINK-PROFILE`.

4 En la sección **Formación de equipos**, haga clic en **Agregar** para agregar una directiva de formación de equipos de asignación de nombres y configure una directiva de **Orden de conmutación por error**.

Se especifica una lista de los vínculos superiores activos y cada interfaz en el nodo de transporte está fijada a un vínculo superior activo. Esta configuración permite el uso de varios vínculos superiores activos al mismo tiempo.

5 Configure vínculos superiores activos y en espera.

Por ejemplo, configure `uplink-1` como el vínculo superior activo y `uplink-2` como el vínculo superior en espera.

6 Introduzca un valor de VLAN de transporte.

El endpoint de túnel (Tunnel Endpoint, TEP) utiliza la VLAN de transporte establecida en el tráfico de superposición de etiquetas de perfil de vínculo superior y el identificador de VLAN.

Por ejemplo, `1060`.

7 Introduzca el valor de MTU.

El valor predeterminado de la MTU del perfil de vínculo superior es 1600.

Nota El valor debe ser al menos 1600, pero no mayor que el valor de MTU en los conmutadores físicos y vSphere Distributed Switch.

Crear un perfil de vínculo superior de Edge

Cree un perfil de vínculo superior con la directiva de formación de equipos de orden de conmutación por error con un vínculo superior activo para el tráfico de superposición de máquinas virtuales de Edge.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Perfiles > Perfiles de vínculo superior > Agregar**.

3 Introduzca un nombre de perfil de enlace ascendente y, de forma opcional, agregue una descripción de perfil de enlace ascendente.

Por ejemplo, `EDGE-UPLINK-PROFILE`.

4 En la sección **Formación de equipos**, haga clic en **Agregar** para agregar una directiva de formación de equipos de asignación de nombres y configure una **directiva de conmutación por error**.

Se enumera una lista de los vínculos superiores activos y cada interfaz en el nodo de transporte está fijada a un vínculo superior activo. Esta configuración permite el uso de varios vínculos superiores activos al mismo tiempo.

5 Configure un vínculo superior activo.

Por ejemplo, configure `uplink-1` como vínculo superior activo.

6 Consulte los vínculos superiores en la página **Perfil de vínculo superior**.

Crear un perfil de nodo de transporte

Un perfil de nodo de transporte define la forma en que se instala y configura NSX-T Data Center en los hosts de un clúster concreto al que está conectado el perfil.

Requisitos previos

Compruebe que se creó una zona de transporte superpuesta.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Perfiles > Perfiles de nodo de transporte > Agregar**.

3 Introduzca un nombre para el perfil de nodo de transporte y, opcionalmente, una descripción.

   Por ejemplo, `HOST-TRANSPORT-NODE-PROFILE`.

4 En la sección **Nuevo conmutador de nodo**, seleccione **Tipo** como `VDS`.

5 Seleccione **Modo** como `Standard`.

6 Seleccione vCenter Server y los nombres del conmutador distribuido de la lista.

   Por ejemplo, `DSwitch`

7 Seleccione la zona de transporte superpuesta creada anteriormente.

   Por ejemplo, `NSX-OVERLAY-TRANSPORTZONE`.

8 Seleccione el perfil de host de vínculo superior creado anteriormente.

   Por ejemplo, `ESXI-UPLINK-PROFILE`.

9 Seleccione **Usar grupo de IP** en la lista **Asignación de IP**.

10 Seleccione el grupo de TEP de host creado anteriormente.

   Por ejemplo, `ESXI-TEP-IP-POOL`.

11 En **Asignación de conmutador de directiva de formación de equipos**, haga clic en el icono de edición y asigne los vínculos superiores definidos en el perfil de vínculo superior de NSX-T a los vínculos superiores de vSphere Distributed Switch.

   Por ejemplo, asigne `uplink-1 (active)` a `Uplink 1` y `uplink-2 (standby)` a `Uplink 2`.

12 Haga clic en **Agregar**.

13 Compruebe que el perfil que creó está incluido en la lista de la página **Perfiles de nodo de transporte**.

Configurar NSX-T Data Center en el clúster

Para instalar NSX-T Data Center y preparar la superposición de TEP, aplique el perfil de nodo de transporte al clúster de vSphere.

Requisitos previos

Compruebe que se creó un perfil de nodo de transporte.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Nodos > Nodos de transporte de host**.

3 En el menú desplegable **Administrado por**, seleccione un vCenter Server existente.

   La página muestra los clústeres de vSphere disponibles.

4 Seleccione el clúster de proceso en el que desea configurar NSX-T Data Center.

5 Haga clic en **Configurar NSX**.

6 Seleccione el perfil de nodo de transporte creado previamente y haga clic en **Aplicar**.

   Por ejemplo, `HOST-TRANSPORT-NODE-PROFILE`.

7 En la página **Nodo de transporte de host**, compruebe que el estado de configuración de NSX-T Data Center sea `Success` y que el estado de conectividad de los hosts en el clúster de NSX Manager sea `Up`.

Resultados

El perfil de nodo de transporte creado anteriormente se aplica al clúster de vSphere para instalar NSX-T Data Center y preparar la superposición de los TEP.

Configurar e implementar un nodo de transporte de NSX Edge

Puede agregar una máquina virtual de NSX Edge al tejido de NSX-T Data Center y proceder a configurarla como una máquina virtual de nodo de transporte de NSX Edge.

Requisitos previos

Compruebe que haya creado las zonas de transporte, el perfil de enlace ascendente de Edge y el grupo de direcciones IP de TEP de Edge.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Nodos > Nodos de transporte de Edge > Agregar máquina virtual de Edge**.

3 En **Nombre y descripción**, escriba un nombre para NSX Edge.

   Por ejemplo, `nsx-edge-1`

4 Introduzca el nombre de host o FQDN de vCenter Server.

   Por ejemplo, `nsx-edge-1.lab.com`.

5 Seleccione el formato `Large`.

6 En **Credenciales**, introduzca la CLI y las contraseñas raíz de NSX Edge. Las contraseñas deben cumplir con las restricciones de seguridad para contraseñas.

   - Al menos 12 caracteres.
   - Al menos una letra en minúsculas.
   - Al menos una letra en mayúsculas.
   - Al menos un dígito.

- Al menos un carácter especial.
- Al menos cinco caracteres diferentes.
- El módulo PAM de Linux aplica las reglas de complejidad de contraseña predeterminadas.

7 Habilite **Permitir inicio de sesión SSH** para las credenciales raíz y de CLI.

8 En **Configurar implementación**, configure las siguientes propiedades:

Opción	Descripción
Administrador de equipo	Seleccione el administrador de equipo en el menú desplegable. Por ejemplo, seleccione `vCenter`.
Clúster	Seleccione el clúster en el menú desplegable. Por ejemplo, seleccione `Compute-Cluster`.
Almacén de datos	Seleccione el almacén de datos compartido de la lista. Por ejemplo, `vsanDatastore`.

9 Configure los ajustes del nodo.

Opción	Descripción
Asignación de IP	Seleccione Estática. Introduzca los valores de: ■ **IP de administración**: introduzca la dirección IP en la misma VLAN que la red de administración de vCenter Server. Por ejemplo, `10.197.79.146/24`. ■ **Puerta de enlace predeterminada**: la puerta de enlace predeterminada de la red de administración. Por ejemplo, `10.197.79.253`.
Interfaz de administración	Haga clic en **Seleccionar interfaz** y, a continuación, seleccione el grupo de puertos de vSphere Distributed Switch en la misma VLAN de la red de administración en el menú desplegable que creó anteriormente. Por ejemplo, `DPortGroup-MGMT`.

10 En **Configurar NSX**, haga clic en **Agregar conmutador** para configurar las propiedades del conmutador.

11 Utilice el nombre predeterminado para el **Nombre del conmutador de Edge**.

Por ejemplo, `nvds1`.

12 Seleccione la zona de transporte a la que pertenece el nodo de transporte.

Seleccione las zonas de transporte superpuestas creadas anteriormente.

Por ejemplo, `nsx-overlay-transportzone`.

13 Seleccione el perfil de vínculo superior de Edge creado anteriormente.

Por ejemplo, `EDGE-UPLINK-PROFILE`.

14 Seleccione **Usar grupo de IP** en **Asignación de IP**.

15 Seleccione el grupo de IP de TEP de Edge creado anteriormente.

Por ejemplo, `EDGE-TEP-IP-POOL`.

16 En la sección **Asignación de conmutador de directiva de formación de equipos**, asigne el vínculo superior a los perfiles de vínculo superior de Edge creados anteriormente.

Por ejemplo, para `Uplink1`, seleccione `DPortGroup-EDGE-TEP`.

17 Repita los pasos 10 a 16 para agregar un conmutador nuevo.

Por ejemplo, configure los siguientes valores:

Propiedad	Valor
Nombre del conmutador de Edge	`nvds2`
Zona de transporte	`nsx-vlan-transportzone`
Perfil de vínculo superior de Edge	`EDGE-UPLINK-PROFILE`
Asignación de conmutador de directiva de formación de equipos	`DPortGroup-EDGE-UPLINK`

18 Haga clic en **Finalizar**.

19 Repita los pasos 2 a 18 para una segunda máquina virtual de NSX Edge.

20 Consulte el estado de conexión en la página **Nodos de transporte de Edge**.

Crear un clúster de NSX Edge

Para asegurarse de que al menos un NSX Edge siempre esté disponible, cree un clúster de NSX Edge.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Sistema > Tejido > Nodos > Clústeres de Edge > Agregar**.

3 Introduzca el nombre del clúster NSX Edge.

Por ejemplo, `EDGE-CLUSTER`.

4 Seleccione el perfil de clúster NSX Edge predeterminado en el menú desplegable.

Seleccione **nsx-default-edge-high-availability-profile**.

5 En el menú desplegable **Tipo de miembro**, seleccione el **nodo de Edge**.

6 En la columna **Disponible**, seleccione las máquinas virtuales de NSX Edge creadas previamente y haga clic en la flecha derecha para moverlas a la columna **Seleccionada**.

7 Por ejemplo, `nsx-edge-1` y `nsx-edge-2`.

8 Haga clic en **Guardar**.

Crear un segmento de vínculo superior de nivel 0

El segmento de vínculo superior de nivel 0 proporciona conectividad de norte a sur desde NSX-T Data Center hasta la infraestructura física.

Requisitos previos

Compruebe que haya creado una puerta de enlace de nivel 0.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Redes > Segmentos > Agregar segmento**.

3 Introduzca un nombre para el segmento.

Por ejemplo, `TIER-0-LS-UPLINK`.

4 Seleccione la zona de transporte creada previamente.

Por ejemplo, seleccione `nsx-vlan-transportzone`.

5 Conmute **Estado de administrador** para habilitarlo.

6 Introduzca un identificador de VLAN de la puerta de enlace de nivel 0.

Por ejemplo, `1089`.

7 Haga clic en **Guardar**.

Crear una puerta de enlace de nivel 0

La puerta de enlace de nivel 0 es el enrutador lógico de NSX-T Data Center que proporciona conectividad de norte a sur para las redes lógicas de NSX-T Data Center a la infraestructura física. vSphere with Tanzu admite varias puertas de enlace de nivel 0 en distintos clústeres de NSX Edge en la misma zona de transporte.

Requisitos previos

Compruebe que se creó un clúster de NSX Edge.

Procedimiento

1 Inicie sesión en NSX Manager.

2 Seleccione **Redes > Puertas de enlace de nivel 0**.

3 Haga clic en **Agregar puerta de enlace de nivel 0**.

4 Introduzca un nombre para la puerta de enlace de nivel 0.

Por ejemplo, `Tier-0_VWT`.

5 Seleccione un modo HA activo-en espera.

En el modo activo-en espera, el miembro activo elegido procesa todo el tráfico. Si se produce un error en el miembro activo, se elige un nuevo miembro para que esté activo.

6 Seleccione el clúster de NSX Edge creado anteriormente.

   Por ejemplo, seleccione `EDGE-CLUSTER`.

7 Haga clic en **Guardar**.

   Se crea la puerta de enlace de nivel 0.

8 Seleccione **Sí** para continuar con la configuración.

9 Configure interfaces.

   a Expanda **Interfaces** y haga clic en **Establezca la opción**.

   b Haga clic en **Agregar interfaz**.

   c Escriba un nombre.

      Por ejemplo, introduzca el nombre `TIER-0_VWT-UPLINK1`.

   d En **Tipo**, seleccione **Externo**.

   e Introduzca una dirección IP del enrutador lógico de Edge – VLAN de vínculo superior. La dirección IP debe ser diferente de la dirección IP de administración configurada para las máquinas virtuales de NSX Edge creadas previamente.

      Por ejemplo, `10.197.154.1/24`.

   f En **Conectado a**, seleccione el segmento de vínculo superior de nivel 0 que creó anteriormente.

      Por ejemplo, `TIER-0-LS-UPLINK`

   g Seleccione un nodo de NSX Edge de la lista.

      Por ejemplo, `nsx-edge-1`.

   h Haga clic en **Guardar**.

   i Repita los pasos de "a" a "h" para la segunda interfaz.

      Por ejemplo, cree un segundo `TIER-0_VWT-UPLINK2` de vínculo superior con la dirección IP `10.197.154.2/24` conectado al nodo de `nsx-edge-2` Edge.

   j Haga clic en **Cerrar.**

10 Para configurar la alta disponibilidad, haga clic en **Establezca la opción** en **Configuración de VIP de alta disponibilidad**.

   a Haga clic en **AGREGAR CONFIGURACIÓN DE VIP DE ALTA DISPONIBILIDAD**.

   b Introduzca la dirección IP.

      Por ejemplo, `10.197.154.3/24`

   c Seleccione las interfaces.

      Por ejemplo, `TIER-0_WVT-UPLINK1` y `TIER-0_WVT-UPLINK2`.

   d Haga clic en **Agregar** y **Aplicar**.

11 Para configurar el enrutamiento, haga clic en **Enrutamiento**.

  a Haga clic en **Establecer** en Rutas estáticas.
  b Haga clic en **AGREGAR RUTA ESTÁTICA**.
  c Escriba un nombre.

    Por ejemplo, `DEFAULT-STATIC-ROUTE`.
  d Introduzca `0.0.0.0/0` para la dirección IP de red.
  e Para configurar los siguientes saltos, haga clic en **Establecer salto siguiente** y, a continuación, en **Agregar salto siguiente**.
  f Introduzca la dirección IP del enrutador del siguiente salto. Suele ser la puerta de enlace predeterminada de la VLAN de la red de administración desde la VLAN de vínculo superior del enrutador lógico de NSX Edge.

    Por ejemplo, `10.197.154.253`.
  g Haga clic en **Agregar**, **Aplicar** y **GUARDAR**.
  h Haga clic en **Cerrar**.

12 Para verificar la conectividad, asegúrese de que un dispositivo externo de la arquitectura física pueda hacer ping en los vínculos superiores que configuró.

Pasos siguientes

Configure clúster supervisor. Consulte Habilitar la administración de cargas de trabajo con redes de NSX-T Data Center.

Configurar redes de vSphere y NSX Advanced Load Balancer para vSphere with Tanzu

vSphere with Tanzu admite NSX Advanced Load Balancer, también conocido como Equilibrador de carga AVI, Essentials Edition y Enterprise Edition. Puede instalar y configurar NSX Advanced Load Balancer 20.1.7 en el entorno de vSphere with Tanzu solo si utiliza redes de vSphere Distributed Switch (VDS) para clúster supervisor.

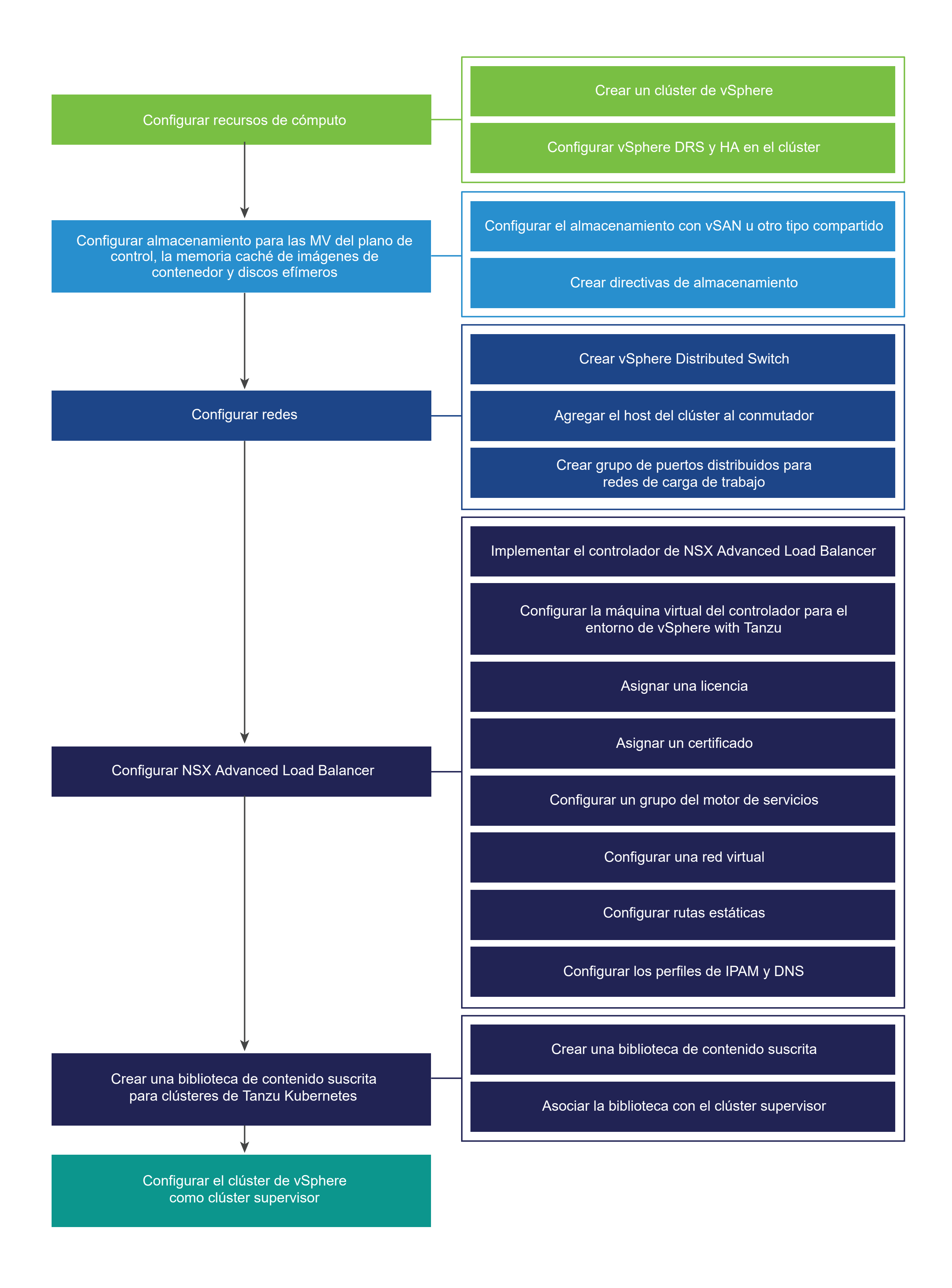
Cómo funciona el equilibrador de carga con clústeres de Tanzu Kubernetes

NSX Advanced Load Balancer proporciona los extremos de equilibrio de carga de escalado dinámico para clústeres de Tanzu Kubernetes aprovisionados por el servicio Tanzu Kubernetes Grid. Instale y configure la máquina virtual del controlador AVI. Cuando haya configurado el controlador, este aprovisiona automáticamente los extremos de equilibrio de carga. Por ejemplo, cuando aprovisiona un clúster de Tanzu Kubernetes, el controlador crea un servicio virtual e implementa una máquina virtual del motor de servicio para alojar ese servicio. Este servicio virtual proporciona equilibrio de carga para el plano de control de Kubernetes.

Cuando se crea un servicio de Kubernetes de tipo equilibrador de carga para ese clúster, el controlador crea automáticamente un servicio virtual y lo implementa en el motor de servicio. El primer motor de servicio solo se crea después de configurar el primer servicio virtual. Todos los servicios virtuales que se configuren posteriormente utilizarán el motor de servicio existente. Puede implementar varios servicios virtuales en una máquina virtual del motor de servicio.

El clúster supervisor con redes de vSphere y el flujo de trabajo de NSX Advanced Load Balancer

Este diagrama muestra el flujo de trabajo para configurar redes de vSphere y NSX Advanced Load Balancer para vSphere with Tanzu.


Configurar recursos de cómputo
Crear un clúster de vSphere
Configurar vSphere DRS y HA en el clúster
Configurar almacenamiento para las MV del plano de control, la memoria caché de imágenes de contenedor y discos efímeros
Configurar el almacenamiento con vSAN u otro tipo compartido
Crear directivas de almacenamiento
Configurar redes
Crear vSphere Distributed Switch
Agregar el host del clúster al conmutador
Crear grupo de puertos distribuidos para redes de carga de trabajo
Configurar NSX Advanced Load Balancer
Implementar el controlador de NSX Advanced Load Balancer
Configurar la máquina virtual del controlador para el entorno de vSphere with Tanzu
Asignar una licencia
Asignar un certificado
Configurar un grupo del motor de servicios
Configurar una red virtual
Configurar rutas estáticas
Configurar los perfiles de IPAM y DNS
Crear una biblioteca de contenido suscrita para clústeres de Tanzu Kubernetes
Crear una biblioteca de contenido suscrita
Asociar la biblioteca con el clúster supervisor
Configurar el clúster de vSphere como clúster supervisor

Procedimiento

1 Componentes de NSX Advanced Load Balancer

Los componentes de NSX Advanced Load Balancer, también conocido como Equilibrador de carga de AVI, incluyen el clúster del Controlador AVI, las máquinas virtuales de los motores de servicio (plano de datos) y el operador de AVI Kubernetes (AKO).

2 Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y NSX Advanced Load Balancer

Para configurar vSphere with Tanzu con el NSX Advanced Load Balancer, también conocido como equilibrador de carga de AVI, el entorno debe cumplir ciertos requisitos. vSphere with Tanzu admite varias topologías para redes AVI: una única red de vDS para los servicios del motor de servicio de AVI y del equilibrador de carga, y un vDS para el plano de administración de AVI y otro vDS para el NSX Advanced Load Balancer.

3 Topología para clúster supervisor con redes de vSphere y NSX Advanced Load Balancer

El controlador AVI siempre se implementa en la red de administración, donde puede establecer una interfaz con vCenter Server, los hosts ESXi y los nodos del plano de control del clúster supervisor. Los motores de servicio se implementan con interfaces en la red de administración y la red de datos.

4 Instalar y configurar el NSX Advanced Load Balancer

Si utiliza redes de vSphere Distributed Switch (VDS), puede instalar y configurar NSX Advanced Load Balancer 20.1.7 en su entorno de vSphere with Tanzu.

Componentes de NSX Advanced Load Balancer

Los componentes de NSX Advanced Load Balancer, también conocido como Equilibrador de carga de AVI, incluyen el clúster del Controlador AVI, las máquinas virtuales de los motores de servicio (plano de datos) y el operador de AVI Kubernetes (AKO).

Controladora

El Controlador AVI, también conocido como el Controlador, interactúa con vCenter Server para automatizar el equilibrio de carga de los clústeres de Tanzu Kubernetes. Se encarga de aprovisionar los motores de servicio, coordinar los recursos entre los motores de servicio y agregar métricas y registros de los motores de servicio. El controlador proporciona una interfaz web, una interfaz de línea de comandos y una API para la operación del usuario y la integración programática.

Después de implementar y configurar la máquina virtual del controlador en vSphere, consulte Implementar un clúster de controladores para obtener información sobre cómo configurar el clúster del plano de control para HA.

Motor de servicio

El motor de servicio AVI, también conocido como motor de servicio, es la máquina virtual del plano de datos. Un motor de servicio ejecuta uno o varios servicios virtuales. El controlador administra un motor de servicio. El controlador aprovisiona los motores de servicio para alojar servicios virtuales.

El motor de servicio tiene dos tipos de interfaces de red:

- La primera interfaz de red, `vnic0` de la máquina virtual, se conecta a la red de administración, donde puede conectarse al Controlador AVI.
- Las restantes interfaces, `vnic1 - 8`, se conectan a la red de datos en la que se ejecutan los servicios virtuales.

Las interfaces del motor de servicio se conectan automáticamente a los grupos de puertos de VDS correctos. Las interfaces no utilizadas se conectan a un grupo de puertos llamado `Avi Internal`, que se crea automáticamente y se reserva para uso futuro. Cada motor de servicio puede admitir hasta 1000 servicios virtuales.

Un servicio virtual proporciona servicios de equilibrio de carga de capa 4 y capa 7 para cargas de trabajo del clúster de Tanzu Kubernetes. Un servicio virtual se configura con una IP virtual y varios puertos. Cuando se implementa un servicio virtual, el controlador selecciona automáticamente una instancia de ESX Server, aumenta la velocidad de giro de un motor de servicio y lo conecta a las redes correctas (grupos de puertos).

El primer motor de servicio solo se crea después de configurar el primer servicio virtual. Todos los servicios virtuales que se configuren posteriormente utilizarán el motor de servicio existente.

Cada servidor virtual expone un equilibrador de carga de capa 4 con una dirección IP distinta del tipo equilibrador de carga para un clúster de Tanzu Kubernetes. La dirección IP asignada a cada servidor virtual se selecciona en el bloque de direcciones IP otorgado al controlador cuando se configura.

AVI es compatible con proveedores de IPAM nativo e IPAM externo. En vSphere, se aprovecha el IPAM nativo de AVI.

Operador de AVI Kubernetes

El operador de AVI Kubernetes (AKO) consulta los recursos de Kubernetes y se comunica con el controlador para solicitar los recursos de equilibrio de carga correspondientes.

El operador de AVI Kubernetes se instala en el clúster supervisor como parte del proceso de habilitación.

Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y NSX Advanced Load Balancer

Para configurar vSphere with Tanzu con el NSX Advanced Load Balancer, también conocido como equilibrador de carga de AVI, el entorno debe cumplir ciertos requisitos. vSphere with Tanzu admite varias topologías para redes AVI: una única red de vDS para los servicios del motor de

servicio de AVI y del equilibrador de carga, y un vDS para el plano de administración de AVI y otro vDS para el NSX Advanced Load Balancer.

Redes de cargas de trabajo

Para configurar un clúster supervisor con la pila de redes de vSphere, debe conectar todos los hosts del clúster a una instancia de vSphere Distributed Switch. En función de la topología que implemente para clúster supervisor, cree uno o varios grupos de puertos distribuidos. Los grupos de puertos se designan como redes de cargas de trabajo para los espacios de nombres de vSphere.

Antes de agregar un host a un clúster supervisor, debe agregarlo a todas las instancias de vSphere Distributed Switch que formen parte del clúster.

Las redes de cargas de trabajo proporcionan conectividad a los nodos de los clústeres de Tanzu Kubernetes y a las máquinas virtuales del plano de control de clúster supervisor. La red de cargas de trabajo que proporciona conectividad a las máquinas virtuales del plano de control de Kubernetes se denomina red de carga de trabajo principal. Cada clúster supervisor debe tener una red de cargas de trabajo principal. Debe designar uno de los grupos de puertos distribuidos como la red de cargas de trabajo principal para clúster supervisor.

Las máquinas virtuales del plano de control de Kubernetes en clúster supervisor usan tres direcciones IP del rango de direcciones IP que se asigna a la red de cargas de trabajo principal. Cada nodo de un clúster de Tanzu Kubernetes tiene una dirección IP independiente asignada desde el rango de direcciones de la red de cargas de trabajo que está configurada con el espacio de nombres en el que se ejecuta el clúster de Tanzu Kubernetes.

Requisitos de red

El NSX Advanced Load Balancer requiere dos subredes que puedan enrutarse:

- Red de administración. La red de administración es donde reside el Controlador AVI, también denominado Controlador. La red de administración proporciona al controlador conectividad con vCenter Server, hosts ESXi y nodos del plano de control del clúster supervisor. Esta red es donde se pone la interfaz de administración del motor de servicio de AVI. Esta red requiere una instancia de vSphere Distributed Switch (vDS) y un grupo de puertos distribuidos.
- Red de datos. La interfaz de datos de los motores de servicio de AVI, también denominados motores de servicio, se conectan a esta red. Las direcciones IP virtuales (VIP) del equilibrador de carga se asignan desde esta red. Esta red requiere una instancia de vSphere Distributed Switch (vDS) y grupos de puertos distribuidos. Debe configurar el vDS y los grupos de puertos antes de instalar el equilibrador de carga.

Asignación de direcciones IP

El controlador y el motor de servicios se conectan a la red de administración. Al instalar y configurar NSX Advanced Load Balancer, proporcione una dirección IP estática y enrutable para cada máquina virtual del controlador.

Los motores de servicio pueden utilizar DHCP. Si DHCP no está disponible, puede configurar un grupo de direcciones IP para los motores de servicio.

Para obtener más información, consulte Configurar puerta de enlace predeterminada.

Requisitos informáticos mínimos

En la tabla se especifican los requisitos informáticos mínimos para las redes de vSphere con NSX Advanced Load Balancer.

Precaución No deshabilite vSphere DRS después de configurar el clúster supervisor. Tener DRS habilitado en todo momento es un requisito previo obligatorio para ejecutar cargas de trabajo en el clúster supervisor. Si se deshabilita DRS, se interrumpirán los clústeres de Tanzu Kubernetes.

Tabla 4-5. Requisitos informáticos mínimos

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
vCenter Server 7.0, 7.0.2, 7.0.3	Pequeño	2	16 GB	290 GB
Hosts ESXi 7.0	3 hosts ESXi con 1 dirección IP estática por host. Si utiliza vSAN: 3 hosts ESXi con al menos 2 NIC físicas es el mínimo; sin embargo, se recomiendan 4 hosts ESXi para conseguir resiliencia durante la aplicación de revisiones y actualizaciones. Los hosts deben unirse a un clúster con vSphere DRS y HA habilitados. vSphere DRS debe estar en el modo Totalmente automatizado o Parcialmente automatizado. **Nota** Asegúrese de que los nombres de los hosts que se unen al clúster utilicen letras minúsculas. De lo contrario, se puede producir un error en la habilitación del clúster para la administración de cargas de trabajo.	8	64 GB por host	No aplicable
Máquinas virtuales de plano de control de Kubernetes	3	4	16 GB	16 GB

Tabla 4-5. Requisitos informáticos mínimos (continuación)

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
Controlador AVI	Essentials	4	12 GB	128 GB
	Enterprise	8	24 GB	128 GB
	Nota Para las implementaciones más pequeñas, puede implementar el controlador de tamaño de Essentials como un único nodo de controlador. Puede crear un clúster de controladores AVI, pero esto no supone ninguna ventaja de rendimiento y anula el propósito de un bajo uso de recursos. En este caso, puede utilizar una copia de seguridad remota para la recuperación ante desastres. Este tamaño solo debe utilizarse con el modo de licencias de AVI Essentials y está limitado a 50 servicios virtuales y 10 motores de servicio. Para los entornos de producción, se recomienda instalar un clúster de 3 máquinas virtuales del Controlador AVI. Se requiere un mínimo de 2 máquinas virtuales del motor de servicio para HA.			
Motor de servicio	Se requiere un mínimo de 2 máquinas virtuales del motor de servicio para HA.	1	2 GB	15 GB

Requisitos mínimos de red

En la tabla se especifican los requisitos de red mínimos para las redes de vSphere con NSX Advanced Load Balancer.

Nota No puede crear clústeres IPv6 con un clúster supervisor de vSphere 7 ni registrar clústeres IPv6 con Tanzu Mission Control. Actualmente, los servicios de NSX Advanced Load Balancer no admiten IPv6.

Tabla 4-6. Requisitos de red mínimos

Componente	Cantidad mínima	Configuración necesaria
IP estáticas para las máquinas virtuales del plano de control de Kubernetes	Bloque de 5	Un bloque de 5 direcciones IP estáticas consecutivas que se asignarán desde la red de administración a las máquinas virtuales del plano de control de Kubernetes en el clúster supervisor.
Red de tráfico de administración	1	Una red de administración que se puede enrutar a los hosts ESXi, a vCenter Server, a la instancia de clúster supervisor y a un equilibrador de carga. La red debe poder acceder a un registro de imágenes y tener conectividad a Internet si el registro de imágenes se encuentra en la red externa. El registro de imágenes se debe poder resolver a través de DNS.
vSphere Distributed Switch 7.0 o posterior	1	Todos los hosts del clúster deben estar conectados a vSphere Distributed Switch.
Redes de cargas de trabajo	1	Se debe crear al menos un grupo de puertos distribuidos en la instancia de vSphere Distributed Switch que se configure como red de cargas de trabajo principal. Según la topología que elija, podrá utilizar el mismo grupo de puertos distribuidos como red de cargas de trabajo de los espacios de nombres o bien podrá crear más grupos de puertos y configurarlos como redes de cargas de trabajo. Las redes de cargas de trabajo deben cumplir los siguientes requisitos: ■ Las redes de cargas de trabajo que se utilizan para el tráfico del clúster de Tanzu Kubernetes deben ser enrutables entre sí y la red de cargas de trabajo principal de clúster supervisor. ■ La función de enrutamiento entre las redes de cargas de trabajo con la red que utiliza NSX Advanced Load Balancer para la asignación de direcciones IP virtuales. ■ No hay superposición de los rangos de direcciones IP en todas las redes de cargas de trabajo dentro de clúster supervisor.
Servidor NTP y DNS	1	Un servidor DNS y un servidor NTP que se pueden utilizar con vCenter Server. **Nota** Configure NTP en todos los hosts ESXi y vCenter Server.

Tabla 4-6. Requisitos de red mínimos (continuación)

Componente	Cantidad mínima	Configuración necesaria
servidor DHCP	1	Opcional. Configure un servidor DHCP para adquirir automáticamente direcciones IP para las redes de administración y cargas de trabajo, así como direcciones IP flotantes. El servidor DHCP debe admitir identificadores de cliente y proporcionar servidores DNS compatibles, dominios de búsqueda de DNS y un servidor NTP. Para la red de administración, todas las direcciones IP, como las direcciones IP de las máquinas virtuales del plano de control, una IP flotante, servidores DNS, DNS, dominios de búsqueda y servidor NTP, se adquieren automáticamente desde el servidor DHCP. clúster supervisor utiliza la configuración de DHCP. Los equilibradores de carga pueden requerir direcciones IP estáticas para la administración. Los ámbitos de DHCP no deben superponerse a estas direcciones IP estáticas. DHCP no se utiliza para direcciones IP virtuales. (VIP)
Subred de red de administración	1	La red de administración es donde reside el Controlador AVI, también denominado Controlador. También es donde se conecta la interfaz de administración del motor de servicio. El Controlador AVI debe conectarse a las direcciones IP de administración de vCenter Server y ESXi desde esta red **Nota** La red de administración y la red de carga de trabajo deben estar en subredes diferentes. No se admite la asignación de la misma subred a las redes de administración y carga de trabajo, lo que puede provocar errores y problemas en el sistema.
Subred de red de datos	1	La interfaz de datos de los motores de servicio de AVI, también denominados motores de servicio, se conectan a esta red. Configure un grupo de direcciones IP para los motores de servicio. Las direcciones IP virtuales (VIP) del equilibrador de carga se asignan desde esta red.
MTU de red física	1.500	El tamaño de MTU debe ser 1500 o superior en cualquier grupo de puertos de vSphere Distributed Switch.
Rango de CIDR del pod de vSphere	/24 direcciones IP privadas	Un rango de CIDR privado que proporciona direcciones IP a los pods de vSphere.

Tabla 4-6. Requisitos de red mínimos (continuación)

Componente	Cantidad mínima	Configuración necesaria
Direcciones IP del controlador AVI	1 o 4	Si implementa el Controlador AVI como un solo nodo, se requiere una dirección IP estática para su interfaz de administración. Para un clúster de 3 nodos, se requieren 4 direcciones IP . Uno para cada máquina virtual del Controlador AVI y otro para la VIP del clúster. Estas direcciones IP deben proceder de la subred de la red de administración.
Rango de VIP de IPAM	-	Un rango de CIDR privado para asignar direcciones IP a los servicios de Kubernetes. Las direcciones IP deben proceder de la subred de la red de datos. Debe especificar un rango de CIDR de servicios de Kubernetes único para cada clúster supervisor.
Servidor NTP y DNS	1	La IP del servidor DNS es necesaria para que el Controlador AVI resuelva correctamente los nombres de host de vCenter Server y ESXi. NTP es opcional, ya que los servidores NTP públicos se utilizan de forma predeterminada.

Puertos y protocolos

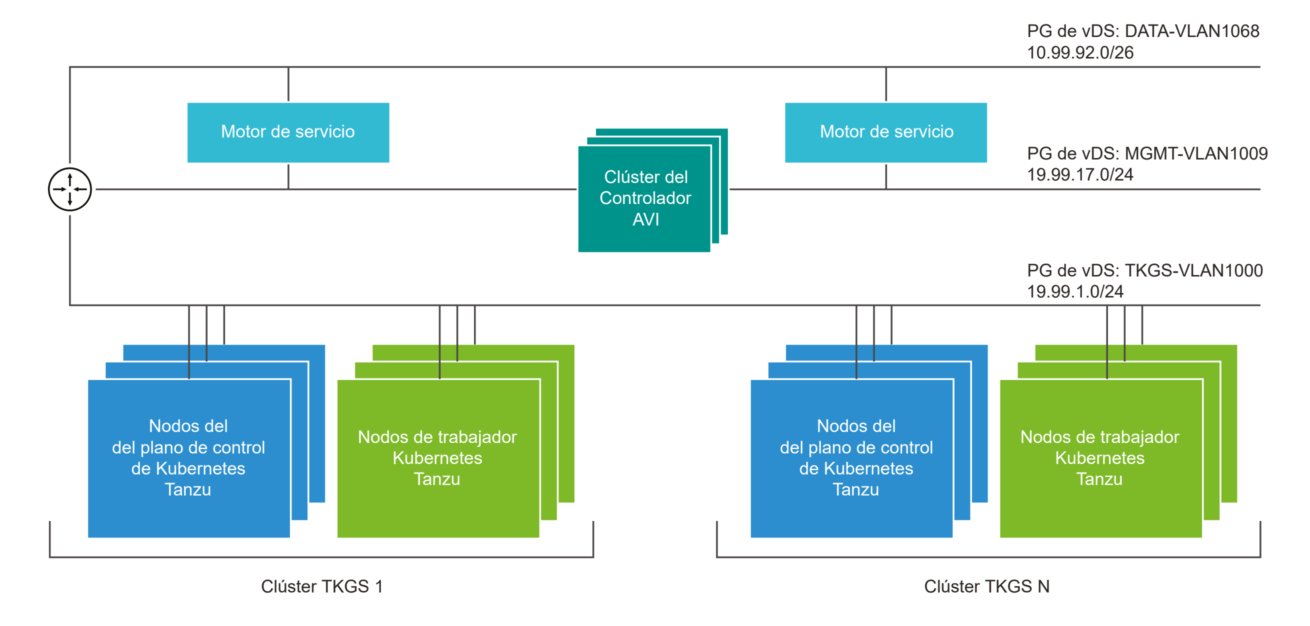
En esta tabla se especifican los protocolos y los puertos necesarios para administrar la conectividad IP entre NSX Advanced Load Balancer, vCenter y otros componentes de vSphere with Tanzu .

Origen	Destino	Protocolo y puertos
Controlador AVI	Controlador AVI (en el clúster)	TCP 22 (SSH) TCP 443 (HTTPS) TCP 8443 (HTTPS)
Motor de servicio	Engine de servicio en HA	TCP 9001 para VMware, LSC y NSX-T Cloud
Motor de servicio	Controlador AVI	TCP 22 (SSH) TCP 8443 (HTTPS) TCP 123 (NTP)
Controlador AVI	vCenter Server, ESXi, NSX-T Manager	TCP 443 (HTTPS)
Nodos del plano de control de supervisor (AKO)	Controlador AVI	TCP 443 (HTTPS)

Para obtener más información sobre los puertos y los protocolos de NSX Advanced Load Balancer, consulte https://ports.esp.vmware.com/home/NSX-Advanced-Load-Balancer.

Topología para clúster supervisor con redes de vSphere y NSX Advanced Load Balancer

El controlador AVI siempre se implementa en la red de administración, donde puede establecer una interfaz con vCenter Server, los hosts ESXi y los nodos del plano de control del clúster supervisor. Los motores de servicio se implementan con interfaces en la red de administración y la red de datos.



La red de administración, como `MGMT-VLAN1009`, es donde se encuentra el controlador y donde se conecta la interfaz de administración de los motores de servicios.

La red de datos, como `DATA-VLAN1068`, es donde se conectan las interfaces del motor de servicio para la colocación de VIP. El tráfico del cliente llega a la VIP y los motores de servicio equilibran la carga del tráfico a las direcciones IP de la red de cargas de trabajo a través de esta red.

La red de cargas de trabajo, como `TKGS-VLAN1000`, es donde se ejecutan los clústeres de Tanzu Kubernetes. Los motores de servicio no requieren interfaces con la red de cargas de trabajo.

Los motores de servicio se ejecutan en modo one-arm. Enrutan el tráfico con equilibrio de carga a la red de cargas de trabajo a través del enrutador. Los motores de servicio no obtienen la IP de puerta de enlace predeterminada de DHCP en las redes de datos. Debe configurar rutas estáticas para que los motores de servicio puedan enrutar el tráfico a las redes de carga de trabajo y la IP del cliente correctamente. Para obtener más información sobre la configuración de rutas estáticas, consulte Configurar puerta de enlace predeterminada.

Esta topología permite que el motor de servicio se encuentre en una sola red y proporcione un servicio de equilibrio de carga a varias redes de carga de trabajo si están presentes. El controlador AVI automatiza la creación del motor de servicio y las conexiones de red.

Instalar y configurar el NSX Advanced Load Balancer

Si utiliza redes de vSphere Distributed Switch (VDS), puede instalar y configurar NSX Advanced Load Balancer 20.1.7 en su entorno de vSphere with Tanzu.

- Compruebe que el entorno cumpla con los requisitos para configurar vSphere with Tanzu con NSX Advanced Load Balancer. Consulte Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y NSX Advanced Load Balancer.
- Descargue el OVA de NSX Advanced Load Balancer. VMware proporciona un archivo OVA de NSX Advanced Load Balancer para que lo implemente en el entorno de vSphere en el que habilitará la administración de cargas de trabajo. Descargue la versión más reciente del archivo OVA compatible con vSphere with Tanzu desde la página de descargas de productos.

Crear una instancia de vSphere Distributed Switch para un clúster supervisor para su uso con NSX Advanced Load Balancer

Para configurar un clúster de vSphere como clúster supervisor que utiliza la pila de redes de vSphere y NSX Advanced Load Balancer, debe crear una instancia de vSphere Distributed Switch. Cree grupos de puertos en el conmutador distribuido que puede configurar como redes de cargas de trabajo en clúster supervisor. NSX Advanced Load Balancer necesita un grupo de puertos distribuidos para conectar las interfaces de datos del motor de servicio de AVI. El grupo de puertos se utiliza para poner las IP virtuales (VIP) de la aplicación en los motores de servicio.

Requisitos previos

Revise los requisitos del sistema y las topologías de red para usar las redes de vSphere para el clúster supervisor con NSX Advanced Load Balancer. Consulte Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y NSX Advanced Load Balancer.

Procedimiento

1. En vSphere Client, desplácese hasta un centro de datos.
2. Haga clic con el botón derecho en el centro de datos y seleccione **Conmutador distribuido > Nuevo conmutador distribuido**.
3. Escriba un nombre para el conmutador, por ejemplo, `Conmutador distribuido de cargas de trabajo`, y haga clic en **Siguiente**.
4. Seleccione la versión 7.0 para el conmutador y haga clic en **Siguiente**.
5. En **Nombre del grupo de puertos**, introduzca `Red de cargas de trabajo principal`, haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.
6. Cree grupos de puertos distribuidos para las redes de cargas de trabajo.
   a. Vaya al conmutador distribuido que se acaba de crear.
   b. Haga clic con el botón derecho en el conmutador y seleccione **Grupo de puertos distribuidos > Nuevo grupo de puertos distribuidos**.

c Escriba un nombre para el grupo de puertos, por ejemplo, **`Red de cargas de trabajo`**, y haga clic en **Siguiente**.

d Deje los valores predeterminados, haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.

7 Cree un grupo de puertos para la red de datos .

a Haga clic con el botón derecho en el conmutador distribuido y seleccione **Grupo de puertos distribuidos > Nuevo grupo de puertos distribuidos**.

b Escriba un nombre para el grupo de puertos, por ejemplo, **`Red de datos`**, y haga clic en **Siguiente**.

c En la página **Configurar parámetros**, introduzca las propiedades generales del nuevo grupo de puertos distribuidos y haga clic en **Siguiente**.

Propiedad	Descripción
Enlace de puertos	Elija cuándo se deben asignar los puertos a las máquinas virtuales conectadas a este grupo de puertos distribuidos. Seleccione **Enlace estático** para asignar un puerto a una máquina virtual cuando la máquina virtual se conecta al grupo de puertos distribuidos.
Asignación de puertos	Seleccione la asignación de puertos **Elástico**. El número predeterminado de puertos es ocho. Cuando se asignan todos los puertos, se crea un nuevo conjunto de ocho puertos.
Cantidad de puertos	Conserve el valor predeterminado .
Grupo de recursos de red	En el menú desplegable, asigne el nuevo grupo de puertos distribuidos a un grupo de recursos de red definido por el usuario . Si no creó un grupo de recursos de red, el menú está vacío.
VLAN	En el menú desplegable, seleccione el tipo de filtrado y marcado del tráfico de VLAN: ■ **Ninguna**: no utilice la VLAN. Seleccione esta opción si utiliza el etiquetado de conmutador externo . ■ **VLAN**: en el cuadro de texto ID de VLAN, escriba un valor de 1 a 4094 para el etiquetado de conmutador virtual. ■ **Enlace troncal de VLAN**: utilice esta opción para el etiquetado de invitado virtual y para pasar el tráfico de VLAN con un identificador al SO invitado. Escriba un rango troncal de VLAN. Puede configurar varios rangos o VLAN individuales con una lista separada por comas. Por ejemplo, `1702-1705`, `1848-1849`. ■ **VLAN privada**: asocie el tráfico a una VLAN privada creada en el conmutador distribuido. Si no creó ninguna VLAN privada, este menú estará vacío.
Avanzado	Deje esta opción sin seleccionar.

8 En la página **Listo para finalizar**, revise la configuración y haga clic en **Finalizar**.

Resultados

Se crea el conmutador distribuido y los grupos de puertos distribuidos aparecen en el conmutador distribuido. Ahora podrá utilizar el grupo de puertos que creó para la red de datos de NSX Advanced Load Balancer.

Implementar el controlador

Implemente la máquina virtual del controlador en la red de administración de su entorno de vSphere with Tanzu.

Requisitos previos

- Compruebe que tiene una red de administración en la que implementar NSX Advanced Load Balancer. Puede ser una instancia de vSphere Distributed Switch (vDS) o un conmutador estándar de vSphere (vSS).
- Compruebe que creó un conmutador vDS y un grupo de puertos para la red de datos. Consulte Crear una instancia de vSphere Distributed Switch para un clúster supervisor para su uso con NSX Advanced Load Balancer.
- Asegúrese de haber completado los requisitos previos. Consulte Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y NSX Advanced Load Balancer.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Seleccione el clúster de vSphere designado para los componentes de administración .

3 Cree un grupo de recursos denominado **`AVI-LB`**.

4 Haga clic con el botón derecho en el grupo de recursos y seleccione **Implementar plantilla de OVF**.

5 Seleccione **Archivo local** y haga clic en **Cargar archivos**.

6 Busque y seleccione el archivo `controller-`*`VERSION`*`.ova` que descargó como requisito previo.

7 Introduzca un nombre y seleccione una carpeta para la controladora.

Opción	Descripción
Nombre de la máquina virtual	**`avi-controller-1`**
Ubicación de la máquina virtual	**Centro de datos**

8 Seleccione el grupo de recursos **`AVI-LB`** como recurso informático.

9 Revise los detalles de la configuración y haga clic en **Siguiente**.

10 Seleccione una **Directiva de almacenamiento de máquina virtual**, como **`vsanDatastore`**.

11 Seleccione la red de administración, como **`MGMT-VLAN1009`**.

12 Personalice la configuración de la siguiente manera y haga clic **Siguiente** cuando haya terminado.

Opción	Descripción
Dirección IP de la interfaz de administración	Introduzca la dirección IP de la máquina virtual del controlador, como **10.999.17.51**.
Máscara de subred de la interfaz de administración	Introduzca la máscara de subred, como **255.255.255.0**.
Puerta de enlace predeterminada	Introduzca la puerta de enlace predeterminada para la red de administración, como **10.199.17.235**.
Clave de autenticación de inicio de sesión de Sysadmim	Pegue el contenido de una clave privada (opcional). Esta es la clave SSH privada que necesita para usar SSH en la máquina virtual. Puede crearlo mediante OpenSSH o PuTTY.

13 Revise la configuración de implementación.

14 Haga clic en **Finalizar** para completar la configuración.

15 Utilice vSphere Client para supervisar el aprovisionamiento de la máquina virtual del controlador en el panel **Tareas**.

16 Utilice vSphere Client para encender la máquina virtual del controlador después de implementarla.

Encender el controlador

Después de implementar la máquina virtual del controlador, podrá encenderla. Durante el proceso de arranque, la dirección IP especificada durante la implementación se asigna a la máquina virtual.

Después de encenderlo, el primer proceso de arranque de la máquina virtual del controlador puede tardar hasta 10 minutos.

Requisitos previos

Implemente el controlador.

Procedimiento

1 En vCenter Server, haga clic con el botón derecho en la máquina virtual `avi-controller-1` que implementó.

2 Seleccione **Encender > Encender**.

A la máquina virtual se le asigna la dirección IP que especificó durante la implementación.

3 Para comprobar si la máquina virtual está encendida, acceda a la dirección IP en un navegador.

Cuando la máquina virtual se conecta, aparecen advertencias sobre el certificado TLS y la conexión.

4 En la advertencia **Esta conexión no es privada**, haga clic en **Mostrar detalles**.

5 Haga clic en **Visitar este sitio web** en la ventana que aparece.

Se le solicitarán las credenciales de usuario.

Configurar el controlador

Configure la máquina virtual del controlador para su entorno de vSphere with Tanzu.

Para conectar el plano de control del equilibrador de carga con el entorno de vCenter Server, el controlador requiere varios parámetros de configuración posteriores a la implementación.

Requisitos previos

- Compruebe que el entorno cumpla con los requisitos del sistema para configurar NSX Advanced Load Balancer. Consulte Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y NSX Advanced Load Balancer.
- Implemente el controlador. Consulte Implementar el controlador.

Procedimiento

1 Con un explorador, diríjase a la dirección IP que especificó al implementar el controlador.

2 Cree una **Cuenta de administrador**.

Opción	Descripción
Nombre de usuario	El nombre de usuario del administrador para la configuración inicial. No puede editar este campo.
Contraseña	Introduzca una contraseña de administrador para la máquina virtual del controlador. La contraseña debe tener al menos 8 caracteres y contener una combinación de caracteres numéricos, caracteres especiales, mayúsculas y minúsculas.
Confirmar contraseña	Vuelva a introducir la contraseña del administrador.
Dirección de correo electrónico (opcional)	Introduzca una dirección de correo electrónico del administrador. Se recomienda proporcionar una dirección de correo electrónico para recuperar la contraseña en un entorno de producción.

3 Ajuste **Configuración del sistema**.

Opción	Descripción
Frase de contraseña	Introduzca una frase de contraseña para la copia de seguridad del controlador. Se realiza una copia de seguridad automática de la configuración del controlador en el disco local de forma periódica. Para obtener más información, consulte Copia de seguridad y restauración. La frase de contraseña debe tener al menos 8 caracteres y contener una combinación de caracteres numéricos, caracteres especiales, mayúsculas y minúsculas.
Confirmar frase de contraseña	Vuelva a introducir la frase de contraseña de copia de seguridad.

Opción	Descripción
Resolutor de DNS	Introduzca una dirección IP para el servidor DNS que está utilizando en el entorno de vSphere with Tanzu. Por ejemplo, `10.14.7.12`.
Dominios de búsqueda de DNS	Introduzca una cadena de dominio.

4 (opcional) Configurar **Correo electrónico/SMTP**

Opción	Descripción
Origen de SMTP	Ninguno, Host local, Servidor SMTP o Servidor anónimo
Dirección de remitente	Dirección de correo electrónico

5 Configure los ajustes de varios tenants.

a Conserve el acceso de tenant predeterminado.

b Seleccione **Configurar nube después de** y haga clic en **Guardar**.

Nota Si no seleccionó la opción **Configurar nube después de** antes de guardar, se cierra el asistente de configuración inicial. La ventana de configuración de la nube no se inicia automáticamente y se le dirige a una vista de panel de control en el controlador. En este caso, desplácese hasta **Infraestructura > Nubes**, edite **Nube predeterminada** y continúe con los siguientes pasos.

6 Configure **Nube predeterminada**.

a Seleccione **Nube**.

b Seleccione **VMware vCenter/vSphere ESX** como el tipo de infraestructura.

7 Configure los ajustes de **Infraestructura**.

Proporcione la información de **inicio de sesión de vCenter/vSphere**.

Opción	Descripción
Nombre de usuario	Introduzca el nombre de usuario del administrador de vCenter, como administrator@vsphere.local. Para usar permisos menores, cree una función dedicada. Consulte Función de usuario de VMware para obtener más información.
Contraseña	Introduzca la contraseña de usuario.
Dirección de vCenter	Escriba el nombre de host o la dirección IP de vCenter Server para el entorno de vSphere with Tanzu.
Permisos de acceso	**Lectura**: cree y administre las máquinas virtuales del motor de servicios. **Escritura**: el controlador crea y administra las máquinas virtuales del motor de servicios. Debe seleccionar Escritura.

Puede dejar los perfiles de IPAM y DNS vacíos.

8 Configure los ajustes del **Centro de datos**.

a Seleccione el **centro de datos** de vSphere donde desea habilitar **Administración de cargas de trabajo**.

b Seleccione el modo **Administración de direcciones IP de red predeterminadas**.

- Seleccione **DHCP habilitado** si DHCP está disponible en los grupos de puertos de vSphere.
- Deje la opción sin seleccionar si desea que las interfaces del motor de servicio utilicen solo direcciones IP estáticas. Puede configurarlos individualmente para cada red.

  Para obtener más información, consulte Configurar una red IP virtual.

c Configure las opciones de **Configuración de ubicación de servicios virtuales**.

Opción	Descripción
Preferir rutas estáticas frente a redes conectadas directamente para la ubicación de servicios virtuales	Seleccione esta opción para forzar que la máquina virtual del motor de servicio acceda a la red del servidor mediante el enrutamiento a través de la puerta de enlace predeterminada. De forma predeterminada, el controlador conecta directamente una NIC a la red del servidor, por lo que debe forzar al motor de servicio a conectarse solo a la red de datos y enrutarse a la red de carga de trabajo.
Usar rutas estáticas para la resolución de red de VIP para la ubicación de servicios virtuales	Deje esta opción sin seleccionar.

9 Configure la **Red** y haga clic en **Guardar**.

Opción	Descripción
Red de administración	Seleccione la red de administración. Los motores de servicio utilizarán esta interfaz de red para conectarse con el controlador. Por ejemplo, `Primary Workload Network`.
Motor de servicio	Deje la plantilla **Grupo de motores de servicio** vacía.
Administración de dirección IP de red de administración:	Seleccione **DHCP habilitado**.

10 (opcional) Configure los siguientes ajustes de red solo si no selecciona **DHCP habilitado**.

Opción	Descripción
Subred IP	Introduzca la subred IP para la red de administración. Por ejemplo, `192.168.110.0/24`. **Nota** Introduzca una subred IP solo si DHCP no está disponible.
Agregar grupo de direcciones IP estáticas	Introduzca una o más direcciones IP o rangos de direcciones IP. Por ejemplo, `192.168.110.66-192.168.110.90`. **Nota** Introduzca una subred IP solo si DHCP no está disponible.
Puerta de enlace predeterminada	Introduzca la puerta de enlace predeterminada de la red de administración, como `192.168.110.1`. **Nota** Introduzca una subred IP solo si DHCP no está disponible.

11 (opcional) Configure los ajustes de NTP si desea utilizar un servidor NTP interno.

a Seleccione **Administración > Configuración > DNS/NTP**.

b Elimine los servidores NTP existentes, si los hubiera, e introduzca la dirección IP del servidor DNS que está utilizando. Por ejemplo, `192.168.100.1`.

Resultados

Una vez completada la configuración, verá **panel de control** del controlador. Seleccione **Infraestructura > Nubes** y compruebe que el estado del controlador de **Nube predeterminada** sea de color verde. A veces, el estado puede ser amarillo durante algún tiempo hasta que el Controlador AVI detecte todos los grupos de puertos en el entorno de vCenter, antes de que cambie a verde.

Agregar una licencia

Cuando haya configurado NSX Advanced Load Balancer, deberá asignarle una licencia. El controlador arranca en modo de evaluación, que dispone de todas las funciones equivalentes a las de una licencia de edición Enterprise. Deberá asignar una licencia Enterprise válida al controlador antes de que caduque su período de evaluación.

Requisitos previos

Compruebe que tiene la licencia de Enterprise.

Procedimiento

1 En el panel de control Controlador AVI, haga clic en el menú situado en la esquina superior izquierda y seleccione **Administración**.

2 Seleccione **Configuración > Licencias**.

3 Para agregar la licencia, seleccione **Cargar desde equipo**.

Después de cargar el archivo de licencia, aparece en la lista de licencias del controlador. El sistema muestra la información sobre la licencia, incluidas la fecha de inicio y la fecha de caducidad.

4 (opcional) Si no dispone de una licencia Enterprise, puede utilizar la edición Essentials.

Nota Si va a cambiar del modo Enterprise o de evaluación a la edición Essentials, deberá realizar el cambio antes de configurar el Controlador AVI. Si ha configurado una función de la edición Enterprise, deberá eliminar los ajustes configurados antes de cambiar a la edición Essentials.

a Seleccione **Configuración > Licencias**.

b Haga clic en el icono de engranaje junto a **Licencias**.

c Seleccione **Licencia de Essentials** y haga clic en **Guardar**.

d Seleccione **Sí** en la ventana emergente para confirmar la edición.

La configuración puede tardar algún tiempo en guardarse y las funciones de Enterprise del Controlador AVI también tardarán en desactivarse.

Implementar un clúster de controladores

De forma opcional, puede implementar un clúster de tres nodos de controlador. Se recomienda configurar un clúster en entornos de producción para HA y recuperación ante desastres. Si va a ejecutar un controlador AVI de un solo nodo, deberá utilizar la función Copia de seguridad y restauración.

Para ejecutar un clúster de tres nodos, después de implementar la primera máquina virtual del controlador, implemente y encienda dos máquinas virtuales del controlador adicionales. No debe ejecutar el asistente de configuración inicial ni cambiar la contraseña de administrador de estos controladores . La configuración de la primera máquina virtual del controlador se asigna a las dos nuevas máquinas virtuales del controlador.

Procedimiento

1 Vaya a **Administración > Controlador**.

2 Seleccione **Nodos**.

3 Haga clic en el icono de edición.

4 Agregue una IP estática para **IP del clúster del controlador**.

Esta dirección IP debe ser de la red de administración .

5 En **Nodos del clúster**, configure los dos nuevos nodos de clúster.

Opción	Descripción
IP	Dirección IP del nodo del controlador .
Nombre	Nombre del nodo. El nombre puede ser la dirección IP .
Contraseña	Contraseña del nodo de controlador . Deje la contraseña vacía.
Dirección IP pública	La dirección IP pública del nodo del controlador . Deje esto vacío.

6 Haga clic en **Guardar**.

Nota Una vez que implemente un clúster, deberá usar la IP del clúster del controlador para cualquier configuración adicional y no la IP del nodo del controlador.

Asignar un certificado al controlador

El controlador debe enviar un certificado a los clientes para establecer una comunicación segura. Este certificado debe tener un nombre alternativo del firmante (SAN) que coincida con el nombre de host o la dirección IP del clúster del Controlador AVI.

El controlador tiene un certificado autofirmado predeterminado. Sin embargo, este certificado no tiene el SAN correcto. Debe reemplazarlo por un certificado válido o autofirmado que tenga el SAN correcto. Puede crear un certificado autofirmado o cargar un certificado externo.

Para obtener más información sobre los certificados, consulte la documentación de AVI.

Procedimiento

1 En el panel de control Controlador AVI, haga clic en el menú de la esquina superior izquierda y seleccione **Plantillas > Seguridad**.

2 Seleccione **Certificado SSL/TLS**.

3 Para crear un certificado, haga clic en **Crear** y seleccione **Certificado de controlador**.

Aparecerá la ventana **Nuevo certificado (SSL/TLS)**.

4 Introduzca un nombre para el certificado.

5 Si no tiene un certificado válido creado previamente, seleccione **Tipo** como `Self Signed` para agregar un certificado autofirmado.

a Introduzca los siguientes detalles:

Opción	Descripción
Nombre común	Especifique el nombre completo del sitio. Para que el sitio se considere de confianza, esta entrada debe coincidir con el nombre de host que introdujo el cliente en el navegador.
Nombre alternativo del sujeto (SAN)	Introduzca la dirección IP o el FQDN del clúster, o ambos, del controlador AVI si se implementa como un solo nodo. Si solo se utiliza la dirección IP o el FQDN, debe coincidir con la dirección IP de la máquina virtual del controlador que especifique durante la implementación. Consulte Implementar el controlador. Introduzca la dirección IP o el FQDN del clúster de la controladora AVI si se implementa como un clúster de tres nodos. Para obtener información sobre la implementación de un clúster de tres nodos de controlador, consulte Implementar un clúster de controladores.
Algoritmo	Seleccione EC (criptografía de curva elíptica) o RSA. Se recomienda la opción EC.
Tamaño de clave	Seleccione el nivel de cifrado que se utilizará para los protocolos de enlace: ■ `SECP256R1` se utiliza para los certificados EC. ■ Se recomienda la opción de 2048 bits para los certificados RSA.

b Haga clic en **Guardar**.

Necesitará este certificado cuando configure el clúster supervisor para habilitar la funcionalidad de administración de cargas de trabajo.

6 Descargue el certificado autofirmado que creó.

a Seleccione **Seguridad > Certificados SSL/TLS**.

Si no ve el certificado, actualice la página.

b Seleccione el certificado que creó y haga clic en el icono de descarga.

c En la página **Exportar certificado** que aparece, haga clic en la opción **Copiar en el portapapeles** del certificado. No copie la clave.

d Guarde el certificado copiado para usarlo más adelante cuando habilite la administración de cargas de trabajo.

7 Si tiene un certificado válido creado previamente, para cargarlo seleccione **Tipo** como `Import`.

   a En **Certificado**, haga clic en **Cargar archivo** e importe el certificado.

      El campo SAN del certificado que cargue debe tener la dirección IP o el FQDN del clúster del controlador.

      Nota Asegúrese de cargar o pegar el contenido del certificado solo una vez.

   b En **Clave (PEM) o PKCS12**, haga clic en **Cargar archivo** e importe la clave.

   c Haga clic en **Validar** para validar el certificado y la clave.

   d Haga clic en **Guardar**.

8 Para cambiar el certificado del portal, realice los siguientes pasos.

   a En el panel de control Controlador AVI, haga clic en el menú de la esquina superior izquierda y seleccione **Administración > Configuración**.

   b Seleccione **Configuración de acceso**.

   c Haga clic en el icono de edición.

   d En **Certificado SSL/TLS**, elimine los certificados del portal predeterminados existentes.

   e En el menú desplegable, seleccione el certificado creado o cargado recientemente.

   f Haga clic en **Guardar**.

Configurar un grupo de motores de servicio

vSphere with Tanzu utiliza el grupo de motores de servicio **Grupo predeterminado**. Opcionalmente, puede configurar los motores de servicio **Grupo predeterminado** dentro de un grupo que defina la colocación y el número de máquinas virtuales de motores de servicio en vCenter. También puede configurar la alta disponibilidad si el controlador de Avi está en modo Enterprise.

Para obtener información sobre cómo aprovisionar la capacidad sobrante en caso de una conmutación por error, consulte la documentación de AVI.

Procedimiento

1 En el panel de control del controlador de Avi, haga clic en el menú de la esquina superior izquierda y, en primer lugar, seleccione **Infraestructura** y, a continuación, seleccione **Recursos de nube**.

2 En la página de configuración, haga clic en **Grupo de motores de servicio**.

3 En la página **Grupo de motores de servicio**, haga clic en el icono Editar en **Grupo predeterminado**.

   Aparece la página **Configuración básica**.

4 En la sección **Configuración de alta disponibilidad y colocación** , seleccione **Modo de alta disponibilidad**.

La opción predeterminada con la licencia de Essentials es `Active/Standby`. Si utiliza la licencia de Enterprise, también puede configurar los modos `Elastic HA N + M Mode` o `Elastic HA Active/Active Mode` .

5 Haga clic en la pestaña **Avanzado**.

6 (opcional) En la sección **Alcance del host y del almacén de datos**, configure los siguientes ajustes:

   a Haga clic en **Incluir** y seleccione el clúster de vSphere en la lista de **Clúster**.

   b Haga clic en **Incluir** y seleccione el clúster de vSphere en la lista de **Host**.

7 (opcional) En la sección **Colocación y HA avanzada**, puede configurar el exceso de capacidad para el grupo de motores de servicio sólo si utiliza la licencia de Enterprise.

Para configurar el exceso de capacidad, especifique un valor en **Motores de servicio del búfer**. El valor que especifique es la cantidad de máquinas virtuales que se implementan para garantizar un exceso de capacidad en caso de una conmutación por error.

Por ejemplo, establezca el valor como `0`.

8 Haga clic en **Guardar**.

Configurar una red IP virtual

Configure una subred IP virtual (VIP) para la red de datos. Puede configurar el rango de VIP que se utilizará cuando se ponga un servicio virtual en la red VIP específica. Puede configurar DHCP para los motores de servicio. Opcionalmente, si DHCP no está disponible, puede configurar un grupo de direcciones IP que se asignarán a la interfaz del motor de servicio de esa red.

Procedimiento

1 En el panel de control Controlador AVI, haga clic en el menú situado en la esquina superior izquierda y seleccione **Infraestructura**.

2 Haga clic en **Red** para mostrar la lista de redes en vCenter Server.

3 Busque la red de datos que proporciona las direcciones IP virtuales y haga clic en el icono Editar para editar la configuración de red.

Por ejemplo, `Data Nework`.

4 Mantenga **DHCP habilitado** seleccionado si DHCP está disponible en la red de datos.

Anule la selección de esta opción si DHCP no está disponible.

5 Anule la selección **Excluir subredes detectadas para la colocación de servicio virtual** . La anulación de la selección de esta opción permite utilizar la subred configurada para la colocación de direcciones IP virtuales.

El Controlador AVI detecta el CIDR de red automáticamente si una máquina virtual se está ejecutando en la red y aparece con el tipo **Detectado**.

6 Si el Controlador AVI detecta la subred IP automáticamente, configure el rango de IP de la subred.

a Haga clic en el icono Editar de la red detectada.

b Seleccione **Agregar grupo de direcciones IP estáticas**.

c Introduzca una o varias direcciones IP o rangos de direcciones IP.

Por ejemplo, `10.202.35.1-10.202.35.254`.

Nota Puede introducir una dirección IP que termine con `0`. Por ejemplo, `192.168.0.0` y omita cualquier advertencia que aparezca.

d Si DHCP está disponible para la dirección IP del motor de servicio, anule la selección de **Utilizar dirección IP estática para VIP y SE** y seleccione **Usar para VIP**.

e Haga clic en **Guardar**.

7 Si el controlador no detecta una subred IP y su tipo, realice los siguientes pasos:

a Haga clic en **Agregar subred**.

b En **Subred IP**, introduzca el CIDR de la red que proporciona las direcciones IP virtuales.

Por ejemplo, `10.202.35.0/22`

c Seleccione **Agregar grupo de direcciones IP estáticas**.

d Introduzca una o varias direcciones IP o rangos de direcciones IP.

El rango debe ser un subconjunto del CIDR de red en **Subred IP**. Por ejemplo, `10.202.35.1-10.202.35.254`.

Nota Puede introducir una dirección IP que termine con `0`. Por ejemplo, `192.168.0.0` y omita cualquier advertencia que aparezca.

e Si DHCP está disponible para la dirección IP del motor de servicio, anule la selección de **Utilizar dirección IP estática para VIP y SE** y seleccione **Usar para VIP**.

f Haga clic en **Guardar** para guardar la configuración de subred.

La página **Editar configuración de red** muestra la subred IP con el tipo **Configurado** y un grupo de direcciones IP.

8 Haga clic en **Guardar** para guardar la configuración de red.

Resultados

La página **Red** muestra las redes configuradas.

Ejemplo

La red `Primary Workload Network` muestra la red detectada como `10.202.32.0/22` y las subredes configuradas como `10.202.32.0/22 [254/254]`. Esto indica que 254 direcciones IP virtuales provienen de `10.202.32.0/22`. Tenga en cuenta que la vista de resumen no muestra los rangos de IP `10.202.35.1-10.202.35.254`.

Configurar puerta de enlace predeterminada

Una puerta de enlace predeterminada permite al motor de servicio enrutar el tráfico a los servidores de grupo en la red de cargas de trabajo. Debe configurar la IP de la puerta de enlace de la red de datos como la puerta de enlace predeterminada.

Procedimiento

1. En el panel de control Controlador AVI, haga clic en el menú de la esquina superior izquierda y seleccione **Infraestructura**.
2. Haga clic en **Enrutamiento**.
3. En la sección **Ruta estática**, haga clic en **Crear**.
4. En **Subred de puerta de enlace**, introduzca `0.0.0.0/0`.
5. En **Salto siguiente**, introduzca la dirección IP de puerta de enlace para la red de datos.

   Por ejemplo, `192.168.0.1`.
6. Haga clic en **Guardar**.

Configurar IPAM

Configure IPAM para el controlador y asígnela a la configuración de nube predeterminada. Actualmente, solo se admite la configuración de nube predeterminada.

Se requiere IPAM para asignar direcciones IP virtuales cuando se crean servicios virtuales.

Procedimiento

1. En el panel de control Controlador AVI, vaya a **Plantillas > Perfiles > Perfiles de IPAM/DNS**.
2. Haga clic en **Crear** y seleccione **Perfil de IPAM** en el menú desplegable.
3. Configure el **Perfil de IPAM**.

Opción	Descripción
Nombre	Cadena definida por el usuario, como **`ipam-profile`**
Tipo	Seleccione **AVI Vantage IPAM**
Asignar IP en VRF	Anule la selección de esta opción.

4 Haga clic en **Agregar red utilizable** y configúrela.

Opción	Descripción
Nube para red utilizable	**Nube predeterminada**
Red utilizable	Seleccione la red IP virtual que configuró.

5 Haga clic en **Guardar**.

`ipam-profile` aparece en la página **Perfiles de IPAM/DNS**.

6 Asigne la IPAM a la configuración de **Nube predeterminada**.

a Vaya a **Infraestructura > Nube**.

b Edite la configuración de **Nube predeterminada**:

Perfil de IPAM: **`ipam-profile`**

c Deje todos los demás valores como predeterminados.

d Haga clic en **Guardar**.

Probar el NSX Advanced Load Balancer

Después de implementar y configurar el plano control de NSX Advanced Load Balancer, compruebe su funcionalidad.

Procedimiento

1 En el panel de la controladora de AVI, vaya a **Infraestructura (Infrastructure) > Nubes (Clouds)**.

2 Compruebe que el estado de la controladora de **Nube predeterminada (Default-Cloud)** esté de color verde.

Para solucionar los problemas que podría encontrar, consulte Solucionar problemas de NSX Advanced Load Balancer.

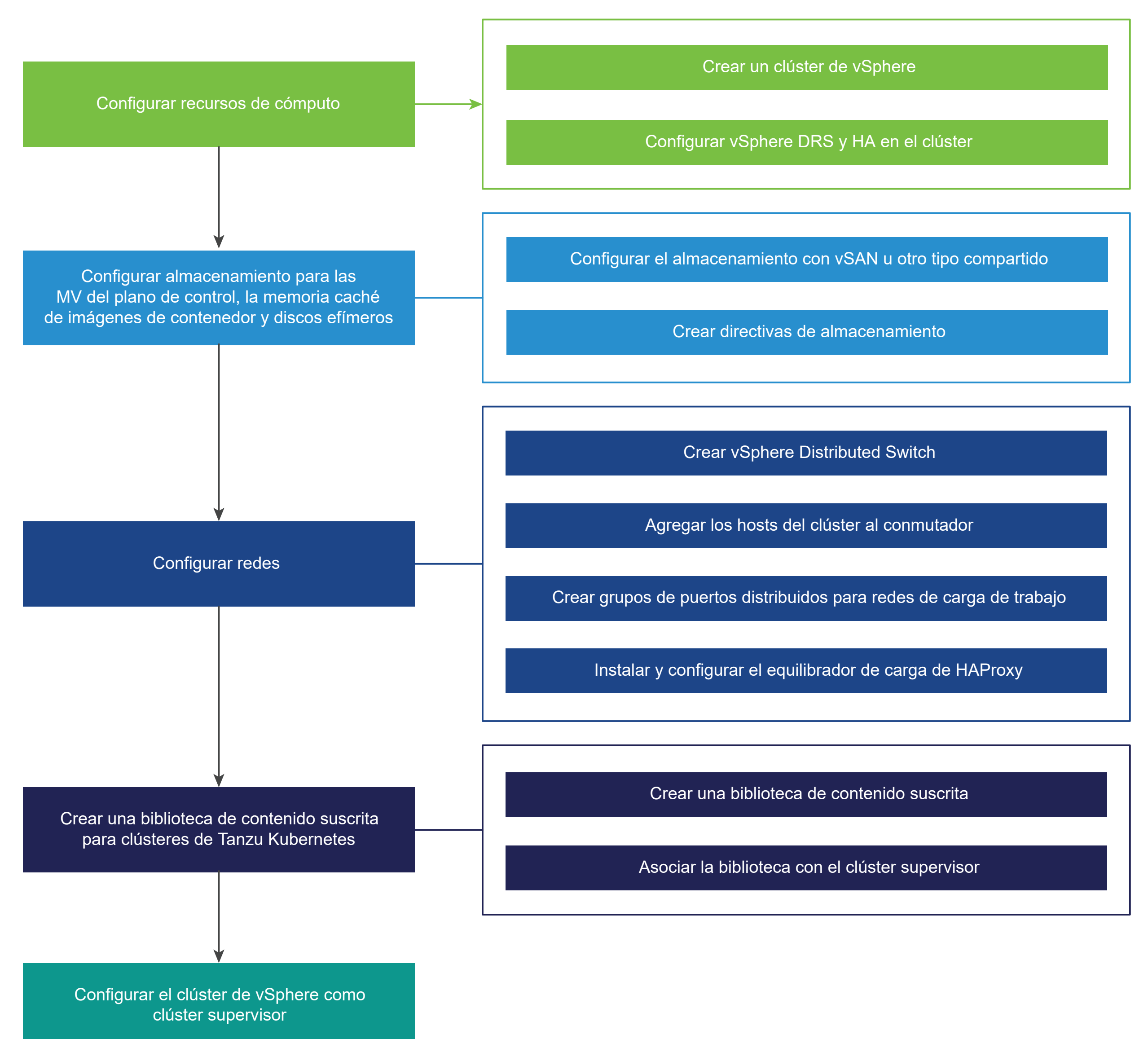
Configurar redes de vSphere y el equilibrador de carga de HAProxy para vSphere with Tanzu

Si utiliza redes de vSphere Distributed Switch para el entorno de vSphere with Tanzu, puede instalar y configurar el equilibrador de carga de HAProxy de código abierto. VMware proporciona una implementación de HAProxy que puede implementar desde un archivo OVA.

clúster supervisor con redes vSphere y flujo de trabajo del equilibrador de carga de HAProxy

Este diagrama muestra el flujo de trabajo para configurar redes de vSphere y el equilibrador de carga de HAProxy para vSphere with Tanzu.

Figura 4-6. Configurar redes de vDS con el flujo de trabajo de HAProxy



Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y el equilibrador de carga de HAProxy

Compruebe los requisitos del sistema para configurar un clúster de vSphere como un clúster supervisor con la pila de redes vSphere y el equilibrador de carga de HAProxy.

Requisitos informáticos mínimos

Sistema	Tamaño de implementación mínimo	CPU	Memoria	Almacenamiento
vCenter Server 7.0	Pequeño	2	16 GB	290 GB
Hosts ESXi 7.0	Sin vSAN: 3 hosts ESXi con 1 dirección IP estática por host. Con vSAN: 4 hosts ESXi con al menos 2 NIC físicas. Los hosts deben unirse a un clúster con vSphere DRS y HA habilitados. vSphere DRS debe estar en el modo Totalmente automatizado o Parcialmente automatizado. **Nota** Asegúrese de que los nombres de los hosts que se unen al clúster utilicen letras minúsculas. De lo contrario, se puede producir un error en la habilitación del clúster para la administración de cargas de trabajo.	8	64 GB por host	No aplicable
Máquinas virtuales de plano de control de Kubernetes	3	4	16 GB	16 GB

Requisitos mínimos de red

Nota No puede crear clústeres IPv6 con un clúster supervisor de vSphere 7 ni registrar clústeres IPv6 con Tanzu Mission Control.

Componente	Cantidad mínima	Configuración necesaria
IP estáticas para las máquinas virtuales del plano de control de Kubernetes	Bloque de 5	Un bloque de 5 direcciones IP estáticas consecutivas que se asignarán a las máquinas virtuales del plano de control de Kubernetes en el clúster supervisor.
Red de tráfico de administración	1	Una red de administración que se puede enrutar a los hosts ESXi, a vCenter Server, a la instancia de clúster supervisor y a un equilibrador de carga. La red debe poder acceder a un registro de imágenes y tener conectividad a Internet si el registro de imágenes se encuentra en la red externa. El registro de imágenes se debe poder resolver a través de DNS.
vSphere Distributed Switch	1	Todos los hosts del clúster deben estar conectados a vSphere Distributed Switch.

Componente	Cantidad mínima	Configuración necesaria
Equilibrador de carga de HAProxy	1	Una instancia del equilibrador de carga de HAProxy configurada con la instancia de vCenter Server. ■ Si la misma instancia de HAProxy se utiliza para múltiples instancias de clúster supervisor, debe poder enrutar el tráfico que se crea hacia todas las redes de cargas de trabajo y desde ellas en todas las instancias de clúster supervisor. Los rangos de IP en todas las redes de cargas de trabajo de todas las instancias de clúster supervisor que atiende HAProxy no deben superponerse. ■ Un rango de IP dedicado para direcciones IP virtuales. La máquina virtual de HAProxy debe ser el único propietario de este rango de IP virtual. El rango no debe superponerse con ningún otro rango de IP asignado a alguna red de cargas de trabajo que sea propiedad de una instancia de clúster supervisor. ■ La red que utiliza HAProxy para asignar direcciones IP virtuales debe enrutarse a las redes de cargas de trabajo que se utilizan en todas las instancias de clúster supervisor a las que se conecta HAProxy.
Redes de cargas de trabajo	1	Se debe crear al menos un grupo de puertos distribuidos en la instancia de vSphere Distributed Switch que se configure como red de cargas de trabajo principal. Según la topología que elija, podrá utilizar el mismo grupo de puertos distribuidos como red de cargas de trabajo de los espacios de nombres o bien podrá crear más grupos de puertos y configurarlos como redes de cargas de trabajo. Las redes de cargas de trabajo deben cumplir los siguientes requisitos: ■ Las redes de cargas de trabajo que se utilizan para el tráfico del clúster de Tanzu Kubernetes deben ser enrutables entre sí y la red de cargas de trabajo principal de clúster supervisor. ■ La función de enrutamiento entre las redes de cargas de trabajo con la red que utiliza HAProxy para la asignación de direcciones IP virtuales. ■ No hay superposición de los rangos de direcciones IP en todas las redes de cargas de trabajo dentro de clúster supervisor. **Importante** La red de carga de trabajo debe estar en una subred diferente a la red de administración.
Servidor NTP y DNS	1	Un servidor DNS y un servidor NTP que se pueden utilizar con vCenter Server. **Nota** Configure NTP en todos los hosts ESXi y vCenter Server.

Componente	Cantidad mínima	Configuración necesaria
servidor DHCP	1	Opcional. Configure un servidor DHCP para adquirir automáticamente direcciones IP para las redes de administración y cargas de trabajo, así como direcciones IP flotantes. El servidor DHCP debe admitir identificadores de cliente y proporcionar servidores DNS compatibles, dominios de búsqueda de DNS y un servidor NTP. clúster supervisor utiliza la configuración de DHCP. Los equilibradores de carga pueden requerir direcciones IP estáticas para la administración. Los ámbitos de DHCP no deben superponerse a estas direcciones IP estáticas. DHCP no se utiliza para direcciones IP virtuales. (VIP)
Subred de red de administración	1	La subred que se utiliza para el tráfico de administración entre los hosts ESXi y vCenter Server y el plano de control de Kubernetes. El tamaño de la subred debe ser el siguiente: ■ Una dirección IP por adaptador de VMkernel de host. ■ Una dirección IP para vCenter Server Appliance. ■ 5 direcciones IP para el plano de control de Kubernetes. 1 para cada uno de los 3 nodos, 1 para la IP virtual, 1 para la actualización sucesiva de clústeres. **Nota** La red de administración y la red de carga de trabajo deben estar en subredes diferentes. No se admite la asignación de la misma subred a las redes de administración y carga de trabajo, lo que puede provocar errores y problemas en el sistema.
VLAN de red de administración	1	Identificador de VLAN de la subred de la red de administración.
MTU de red física	1.600	El tamaño de MTU debe ser 1600 o superior en cualquier red que transporte tráfico superpuesto.
Rango de CIDR de servicios de Kubernetes	/16 direcciones IP privadas	Un rango de CIDR privado para asignar direcciones IP a los servicios de Kubernetes. Debe especificar un rango de CIDR único de servicios de Kubernetes para cada clúster supervisor.

Topologías para implementar el equilibrador de carga de HAProxy

Al usar vSphere with Tanzu con redes de vDS, HAProxy brinda equilibrio de carga para desarrolladores que acceden al plano de control de Tanzu Kubernetes y para los servicios de Kubernetes del tipo equilibrador de carga. Revise las topologías posibles que puede implementar para el equilibrador de carga de HAProxy.

Redes de carga de trabajo en el clúster supervisor

Para configurar una instancia de clúster supervisor con la pila de redes de vSphere, debe conectar todos los hosts del clúster a una instancia de vSphere Distributed Switch. En función de la topología que implemente para las redes de carga de trabajo de clúster supervisor, cree uno o varios grupos de puertos distribuidos. Los grupos de puertos se designan como redes de cargas de trabajo para los espacios de nombres de vSphere.

Antes de agregar un host a un clúster supervisor, debe agregarlo a todas las instancias de vSphere Distributed Switch que formen parte del clúster.

Las redes de cargas de trabajo proporcionan conectividad a los nodos de los clústeres de Tanzu Kubernetes y a las máquinas virtuales del plano de control de clúster supervisor. La red de cargas de trabajo que proporciona conectividad a las máquinas virtuales del plano de control de Kubernetes se denomina red de carga de trabajo principal. Cada clúster supervisor debe tener una red de cargas de trabajo principal. Debe designar uno de los grupos de puertos distribuidos como la red de cargas de trabajo principal para clúster supervisor.

Nota Las redes de carga de trabajo solo se agregan cuando habilita el clúster supervisor y no se pueden agregar más adelante.

Las máquinas virtuales del plano de control de Kubernetes en clúster supervisor usan tres direcciones IP del rango de direcciones IP que se asigna a la red de cargas de trabajo principal. Cada nodo de un clúster de Tanzu Kubernetes tiene una dirección IP independiente asignada desde el rango de direcciones de la red de cargas de trabajo que está configurada con el espacio de nombres en el que se ejecuta el clúster de Tanzu Kubernetes.

Asignación de rangos de direcciones IP

Cuando planifique la topología de red de clúster supervisor con el equilibrador de carga de HA Proxy, planee tener dos tipos de rangos de direcciones IP:

- Un rango para asignar direcciones IP virtuales para HAProxy. El rango de IP que se configura para los servidores virtuales de HAProxy está reservado por el dispositivo del equilibrador de carga. Por ejemplo, si el rango de direcciones IP virtuales es `192.168.1.0/24`, no se podría acceder a todos los hosts de ese rango para otro tráfico que no sea el tráfico de IP virtual.

  Nota No debe configurar una puerta de enlace dentro del rango de direcciones IP virtuales de HAProxy, ya que se podrían generar errores en todas las rutas a esa puerta de enlace.

- Un rango de direcciones IP para los nodos de clúster supervisor y los clústeres de Tanzu Kubernetes. Cada máquina virtual del plano de control de Kubernetes en clúster supervisor tiene asignada una dirección IP, lo que supone un total de tres direcciones IP. Cada nodo de un clúster de Tanzu Kubernetes también tiene asignada una dirección IP independiente. Debe asignar un rango de direcciones IP único a cada red de cargas de trabajo en el clúster supervisor que configure en un espacio de nombres.

Ejemplo de una configuración con una red de /24:

- Red: 192.168.120.0/24

- VIP de HAProxy: 192.168.120.128/25
- 1 dirección IP para la interfaz de carga de trabajo de HAProxy: 192.168.120.5

En función de las direcciones IP que estén libres en las primeras 128 direcciones, puede definir rangos de IP para las redes de cargas de trabajo en clúster supervisor, por ejemplo:

- 192.168.120.31-192.168.120.40 para la red de cargas de trabajo principal
- 192.168.120.51-192.168.120.60 para otra red de cargas de trabajo

Nota Los rangos que defina para las redes de cargas de trabajo no deben superponerse con el rango de VIP de HAProxy.

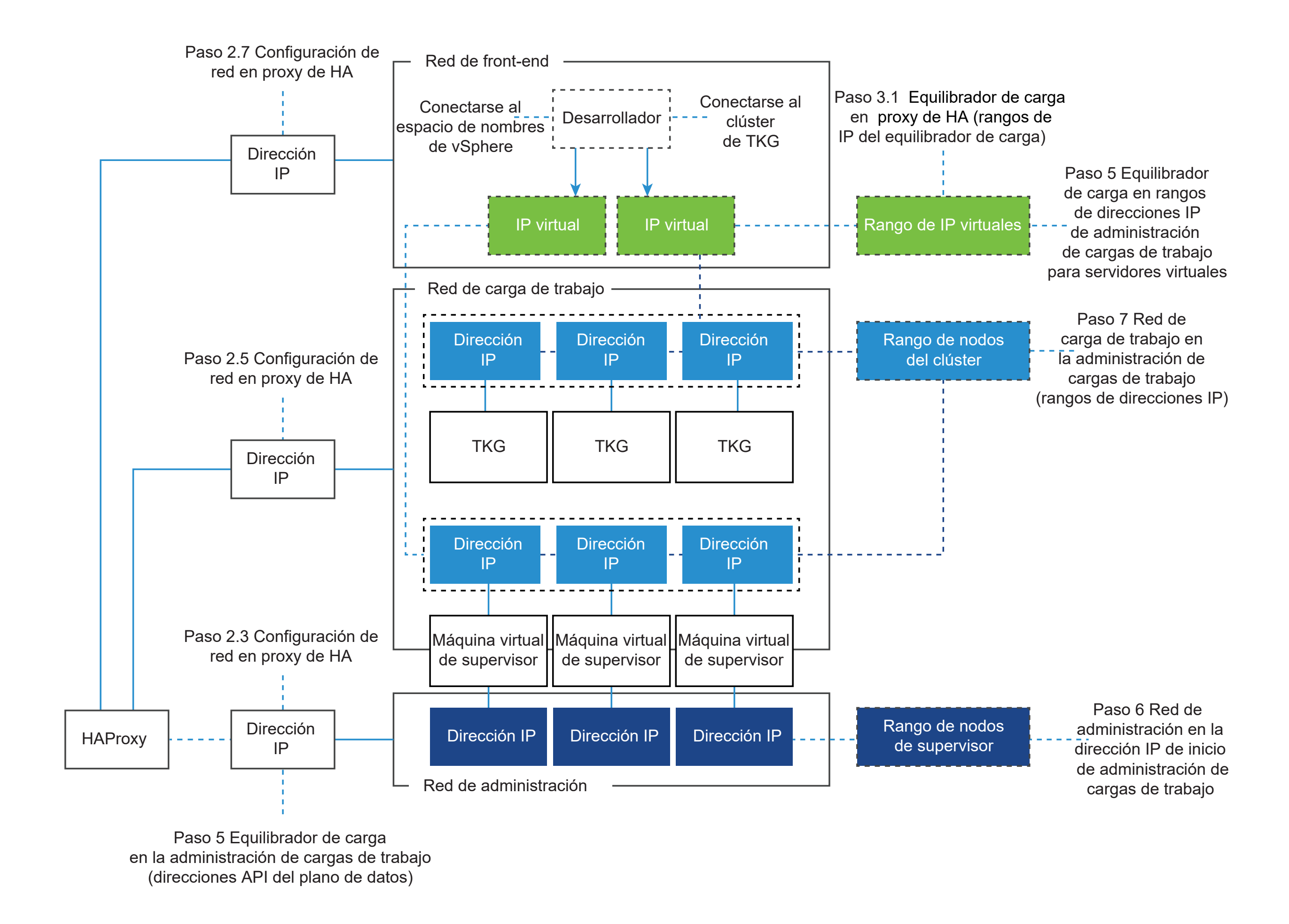
Topología de red de HAProxy

Existen dos opciones de configuración de red para implementar HAProxy: **Predeterminada** y **Front-end**. La red predeterminada tiene 2 NIC: una para la red de administración y otra para la red de cargas de trabajo. La red de front-end tiene 3 NIC: red de administración, red de cargas de trabajo y red de front-end para los clientes. En la tabla se enumeran y describen las características de cada red.

En el caso de las instalaciones de producción, se recomienda implementar el equilibrador de carga de HAProxy con la configuración de **Red de front-end**. Si implementa el equilibrador de carga de HAProxy con la configuración **Predeterminada**, se recomienda asignar un tamaño de bloque de direcciones IP de /24 a la red de cargas de trabajo. Para ambas opciones de configuración, no se recomienda utilizar DHCP.

Red	Características
Administración	El clúster supervisor utiliza la red de administración para conectarse al equilibrador de carga de HAProxy y programarlo. - El endpoint de la API del plano de datos de HAProxy está enlazado a la interfaz de red conectada a la red de administración. - La dirección IP de administración asignada a la máquina virtual del plano de control de HAProxy debe ser una dirección IP estática en la red de administración, de modo que el clúster supervisor pueda conectarse con confianza a la API del equilibrador de carga. - La puerta de enlace predeterminada de la máquina virtual de HAProxy debe estar en esta red. - Las consultas de DNS deben realizarse en esta red.
Carga de trabajo	La máquina virtual del plano de control de HAProxy utiliza la red de cargas de trabajo para acceder a los servicios de los nodos del clúster supervisor y del clúster de Tanzu Kubernetes. - La máquina virtual del plano de control de HAProxy reenvía el tráfico a los nodos del clúster supervisor y del clúster de Tanzu Kubernetes en esta red. - Si la máquina virtual del plano de control de HAProxy se implementa en el modo predeterminado (dos NIC), la red de cargas de trabajo debe proporcionar las redes lógicas que se utilizarán para acceder a los servicios del equilibrador de carga. - En la configuración **Predeterminada**, las direcciones IP virtuales del equilibrador de carga y las direcciones IP del nodo del clúster de Kubernetes proceden de esta red. Se definirán como rangos independientes que no se superponen dentro de la red. **Nota** La red de carga de trabajo debe estar en una subred diferente a la red de administración. Consulte los Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y el equilibrador de carga de HAProxy.
Front-end (opcional)	Los clientes externos (como usuarios o aplicaciones) que acceden a las cargas de trabajo del clúster usan la red de front-end para acceder a los servicios con carga equilibrada del back-end mediante direcciones IP virtuales. - La red de front-end solo se utiliza cuando la máquina virtual del plano de control de HAProxy se implementa con tres NIC. - Esta opción se recomienda para instalaciones de producción. - La red de front-end es donde muestra la dirección IP virtual (VIP). HAProxy equilibrará y reenviará el tráfico al back-end adecuado.

En el siguiente diagrama se muestra una implementación de HAProxy con una topología de **red de front-end**. El diagrama indica dónde se espera que estén los campos de configuración durante el proceso de instalación y configuración.



Topología de clúster supervisor con una red de carga de trabajo y HA Proxy con dos NIC virtuales

En esta topología, se configura un clúster supervisor con una red de carga de trabajo para los siguientes componentes:

- Máquinas virtuales de plano de control de Kubernetes
- Los nodos de los clústeres de Tanzu Kubernetes.
- El rango de IP virtuales de HAProxy donde se conectan los servicios externos y los usuarios de desarrollo y operaciones. En esta configuración, HAProxy se implementa con dos NIC virtuales (configuración **Predeterminada**), una conectada a la red de administración y otra conectada a la red de cargas de trabajo principal. Debe planificar la asignación de direcciones IP virtuales en una subred independiente de la red de cargas de trabajo principal.

Designe un grupo de puertos como red de cargas de trabajo principal para el clúster supervisor y, a continuación, utilice el mismo grupo de puertos como red de cargas de trabajo para los espacios de nombres de vSphere. El clúster supervisor, los clústeres de Tanzu Kubernetes, HAProxy, los usuarios de desarrollo y operaciones y los servicios externos se conectan al mismo grupo de puertos distribuidos que se establece como red de cargas de trabajo principal.

Figura 4-7. clúster supervisor respaldado por una red

La ruta de tráfico para los usuarios de desarrollo y operaciones o las aplicaciones externas es la siguiente:

1 El usuario de desarrollo y operaciones o el servicio externo envían tráfico a una dirección IP virtual en la subred de red de cargas de trabajo del grupo de puertos distribuidos.

2 HAProxy equilibra la carga del tráfico de IP virtual con la dirección IP del nodo de Tanzu Kubernetes o la dirección IP de la máquina virtual del plano de control. HAProxy reclama la dirección IP virtual para que pueda equilibrar la carga del tráfico que entra en esa IP.

3 La máquina virtual del plano de control o el nodo del clúster de Tanzu Kubernetes entrega el tráfico a los pods de destino que se ejecutan dentro del clúster supervisor o el clúster de Tanzu Kubernetes, respectivamente.

Topología de clúster supervisor con una red de carga de trabajo aislada y HA Proxy con dos NIC virtuales

En esta topología, se configuran redes para los siguientes componentes:

- Máquinas virtuales del plano de control de Kubernetes. Una red de cargas de trabajo principal para controlar el tráfico de las máquinas virtuales del plano de control de Kubernetes.

- Nodos del clúster de Tanzu Kubernetes. Una red de cargas de trabajo. que asigna a todos los espacios de nombres del clúster supervisor. Esta red conecta los nodos del clúster de Tanzu Kubernetes.
- IP virtuales de HAProxy. En esta configuración, la máquina virtual de HAProxy se implementa con dos NIC virtuales (configuración **Predeterminada**). Puede conectar la máquina virtual de HAProxy a la red de cargas de trabajo principal o a la red de cargas de trabajo que utiliza para los espacios de nombres. También puede conectar HAProxy a una red de máquinas virtuales que ya exista en vSphere y que se pueda enrutar a las redes principal y de cargas de trabajo.

El clúster supervisor está conectado al grupo de puertos distribuidos que respalda la red de cargas de trabajo principal y los clústeres de Tanzu Kubernetes están conectados a un grupo de puertos distribuidos que respalda la red de cargas de trabajo. Los dos grupos de puertos deben ser enrutables de capa 3. El aislamiento de la capa 2 se puede implementar a través de las VLAN. El filtrado de tráfico de la capa 3 es posible a través de las puertas de enlace y los firewalls de IP.

Figura 4-8. clúster supervisor con una red de cargas de trabajo aislada

La ruta de tráfico para el servicio externo o los usuarios de desarrollo y operaciones es la siguiente:

1. El servicio externo o el usuario de desarrollo y operaciones envía tráfico a una dirección IP virtual. El tráfico se enruta a la red donde se conecta HAProxy.
2. HAProxy equilibra la carga del tráfico de IP virtual con la dirección IP del nodo de Tanzu Kubernetes o la máquina virtual del plano de control. HAProxy reclama la dirección IP virtual para que pueda equilibrar la carga del tráfico que entra en esa IP.

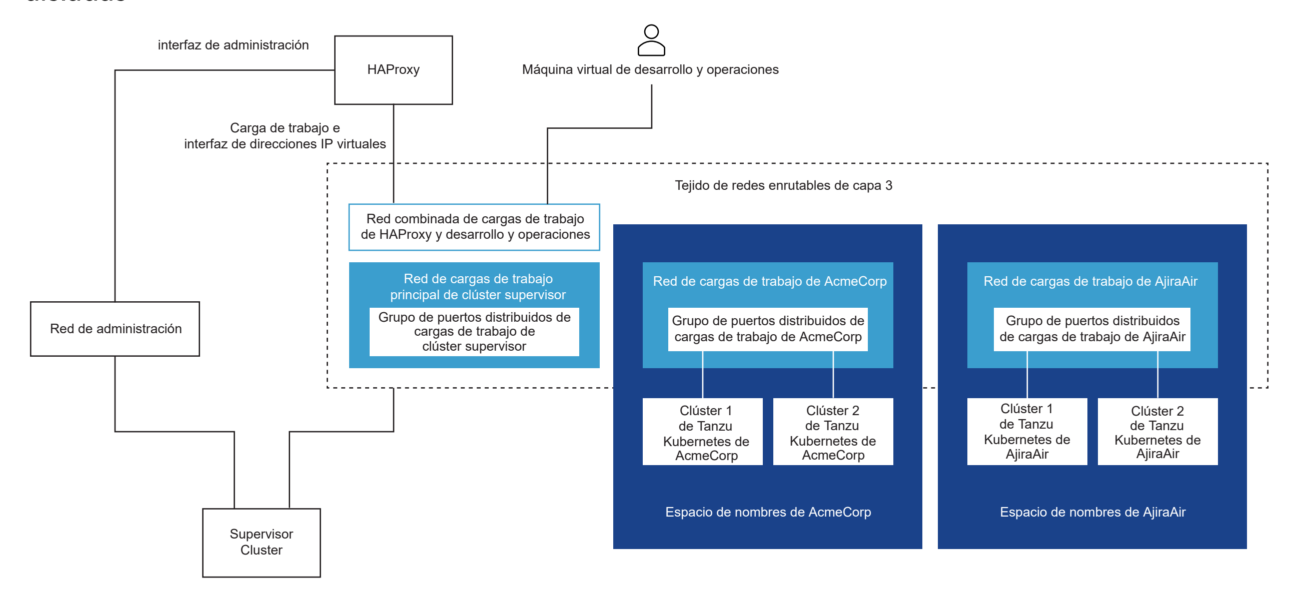
3 La máquina virtual del plano de control o el nodo del clúster de Tanzu Kubernetes entrega el tráfico a los pods de destino que se ejecutan dentro del clúster de Tanzu Kubernetes.

Topología de clúster supervisor con una red de carga de trabajo múltiple y HA Proxy con dos NIC virtuales

En esta topología, es posible configurar un grupo de puertos para que actúe como red de cargas de trabajo principal y un grupo de puertos dedicados que sirvan como red de cargas de trabajo para cada espacio de nombres. HAProxy se implementa con dos NIC virtuales (configuración **Predeterminada**) y puede conectarse a la red de cargas de trabajo principal o a cualquiera de las redes de cargas de trabajo. También puede utilizar una red de máquinas virtuales existente que se pueda enrutar a las redes principal y de cargas de trabajo.

La ruta de tráfico para los servicios externos o los usuarios de desarrollo y operaciones en esta topología es la misma que la de la topología de red de cargas de trabajo aislada.

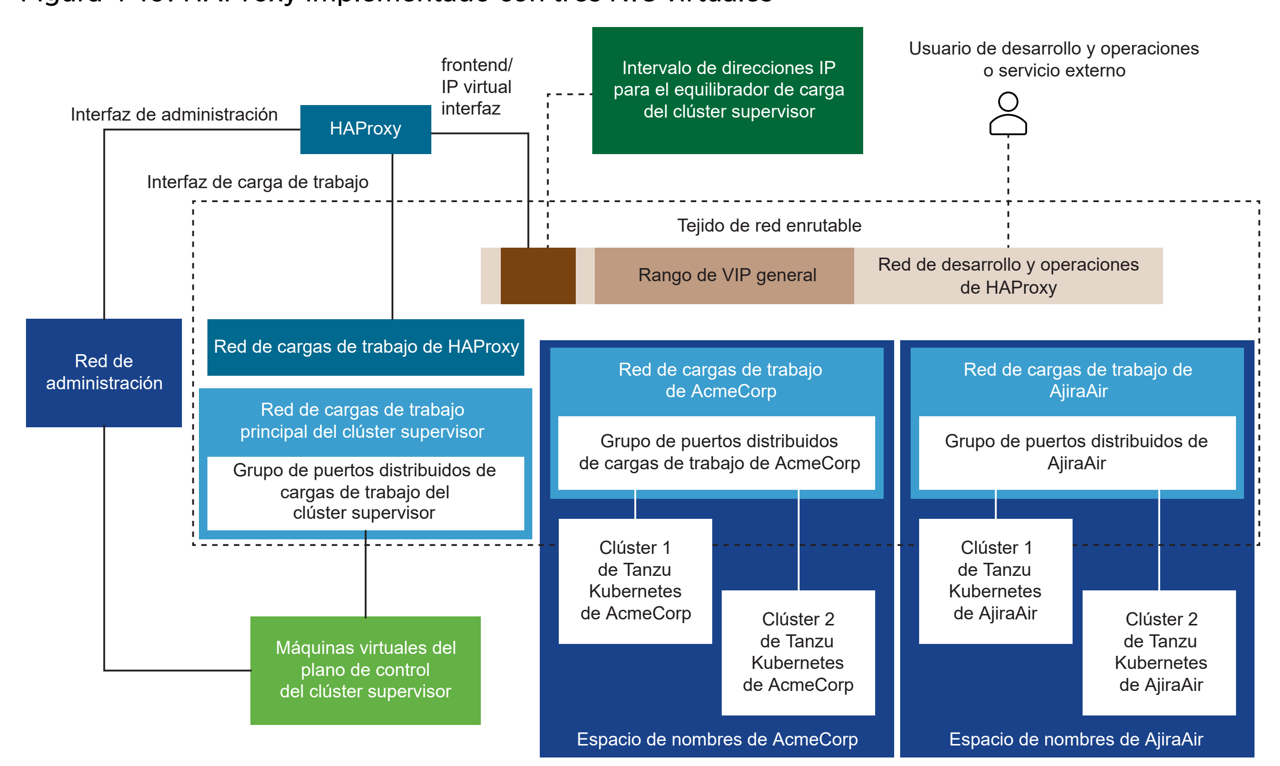
Figura 4-9. Instancia de clúster supervisor respaldada por varias redes de cargas de trabajo aisladas



Topología de clúster supervisor con una red de carga de trabajo múltiple y HA Proxy con tres NIC virtuales

En esta configuración, se implementa la máquina virtual de HAProxy con tres NIC virtuales, por lo que HAProxy se conecta a una red de front-end. Los usuarios y los servicios externos de desarrollo y operaciones pueden acceder a HAProxy a través de IPs virtuales en la red front-end. Se recomienda implementar HA Proxy con tres NIC virtuales para entornos de producción.

Figura 4-10. HAProxy implementado con tres NIC virtuales



Seleccionar entre las posibles topologías

Antes de seleccionar alguna de las posibles topologías, debe evaluar las necesidades de su entorno:

1 ¿Necesita el aislamiento de Capa 2 entre el clúster supervisor y los clústeres de Tanzu Kubernetes?

   a No: la topología más simple, con una red de cargas de trabajo que atienda a todos los componentes.

   b Sí: la topología de red de cargas de trabajo aislada con redes principal y de cargas de trabajo independientes.

2 ¿Necesita aún más aislamiento de Capa 2 entre los clústeres de Tanzu Kubernetes?

   a No: topología de red de cargas de trabajo aislada con redes principal y de cargas de trabajo independientes.

   b Sí: topología con varias redes de cargas de trabajo con una red de cargas de trabajo independiente para cada espacio de nombres y una red de cargas de trabajo principal dedicada.

3 ¿Desea evitar que los usuarios de desarrollo y operaciones y los servicios externos enruten directamente a las máquinas virtuales del plano de control de Kubernetes y los nodos del clúster de Tanzu Kubernetes?

   a No: configuración de HAProxy con dos NIC.

b Sí: configuración de HAProxy con tres NIC Esta configuración se recomienda para entornos de producción.

Crear una instancia de vSphere Distributed Switch para un clúster supervisor para su uso con el equilibrador de carga de HAProxy

Para configurar un clúster de vSphere como un clúster supervisor que utiliza la pila de redes de vSphere y el equilibrador de carga de HAProxy, debe agregar los hosts a una instancia de vSphere Distributed Switch. Debe crear grupos de puertos en el conmutador distribuido que configurará como redes de cargas de trabajo en clúster supervisor.

Puede seleccionar entre diferentes topologías para clúster supervisor en función del nivel de aislamiento que desee proporcionar a las cargas de trabajo de Kubernetes que se ejecutarán en el clúster.

Requisitos previos

- Revise los requisitos del sistema para usar redes de vSphere para el clúster supervisor con el equilibrador de carga de HAProxy. Consulte Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y el equilibrador de carga de HAProxy.
- Determine la topología para configurar redes de cargas de trabajo con HAProxy en el clúster supervisor. Consulte Topologías para implementar el equilibrador de carga de HAProxy.

Procedimiento

1 En vSphere Client, desplácese hasta un centro de datos.

2 Haga clic con el botón derecho en el centro de datos y seleccione **Conmutador distribuido > Nuevo conmutador distribuido**.

3 Escriba un nombre para el conmutador, por ejemplo, `Conmutador distribuido de cargas de trabajo`, y haga clic en **Siguiente**.

4 Seleccione la versión 7.0 para el conmutador y haga clic en **Siguiente**.

5 En **Nombre del grupo de puertos**, introduzca `Red de cargas de trabajo principal`, haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.

   Se creará un conmutador distribuido nuevo con un grupo de puertos en el centro de datos. Este grupo de puertos se podrá utilizar como la red de cargas de trabajo principal de la instancia de clúster supervisor que creará. La red de cargas de trabajo principal controla el tráfico de las máquinas virtuales del plano de control de Kubernetes.

6 Cree grupos de puertos distribuidos para las redes de cargas de trabajo.

   La cantidad de grupos de puertos que cree dependerá de la topología que desee implementar para clúster supervisor. Para una topología con una red de cargas de trabajo aislada, cree un

grupo de puertos distribuidos que se utilizará como red para todos los espacios de nombres en clúster supervisor. En el caso de una topología con redes aisladas para cada espacio de nombres, cree la misma cantidad de grupos de puertos que de los espacios de nombres que creará.

a Vaya al conmutador distribuido que se acaba de crear.

b Haga clic con el botón derecho en el conmutador y seleccione **Grupo de puertos distribuidos > Nuevo grupo de puertos distribuidos**.

c Escriba un nombre para el grupo de puertos, por ejemplo, **`Red de cargas de trabajo`**, y haga clic en **Siguiente**.

d Deje los valores predeterminados, haga clic en **Siguiente** y, a continuación, haga clic en **Finalizar**.

7 Agregue los hosts de los clústeres de vSphere que vaya a configurar como clúster supervisor en el conmutador distribuido.

a Haga clic con el botón derecho en el conmutador distribuido y seleccione **Agregar y administrar hosts**.

b Seleccione **Agregar hosts**.

c Haga clic en **Nuevos hosts**, seleccione los hosts del clúster de vSphere que vaya a configurar como clúster supervisor y haga clic en **Siguiente**.

d Seleccione una NIC física de cada host y asígnele un vínculo superior en el conmutador distribuido.

e Haga clic en **Siguiente** en las pantallas del asistente que irán apareciendo y, por último, haga clic en **Finalizar**.

Resultados

Se agregarán los hosts al conmutador distribuido. Ahora podrá utilizar los grupos de puertos que cree en el conmutador como redes de cargas de trabajo de clúster supervisor.

Instalar y configurar el equilibrador de carga de HAProxy

VMware proporciona una implementación del equilibrador de carga de HAProxy de código abierto que se puede usar en el entorno de vSphere with Tanzu. Si utiliza redes de vSphere Distributed Switch (vDS) para la **administración de cargas de trabajo**, puede instalar y configurar el equilibrador de carga de HAProxy.

Implementar la máquina virtual del plano de control del equilibrador de carga de HAProxy

Si desea utilizar la pila de redes de vSphere para cargas de trabajo de Kubernetes, instale la máquina virtual del plano de control de HAProxy para proporcionar servicios de equilibrio de carga a los clústeres de Tanzu Kubernetes.

Requisitos previos

- Compruebe que el entorno cumpla con los requisitos informáticos y de red para implementar HAProxy. Consulte Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y el equilibrador de carga de HAProxy.
- Compruebe si tiene una red de administración en el conmutador estándar o distribuido de vSphere en el que se va a implementar el equilibrador de carga de HAProxy. El clúster supervisor se comunica con el equilibrador de carga de HAProxy en esa red de administración.
- Cree una instancia de vSphere Distributed Switch y grupos de puertos para redes de cargas de trabajo. El equilibrador de carga de HAProxy se comunica con los nodos del clúster supervisor y del clúster de Tanzu Kubernetes a través de las redes de cargas de trabajo. Consulte Crear una instancia de vSphere Distributed Switch para un clúster supervisor para su uso con el equilibrador de carga de HAProxy. Para obtener más información sobre las redes de cargas de trabajo, consulte Redes de carga de trabajo en el clúster supervisor.
- Descargue la versión más reciente del archivo OVA de VMware HAProxy desde el sitio de VMware-HAProxy.
- Seleccione una topología para implementar el equilibrador de carga de HAProxy y las redes de cargas de trabajo en el clúster supervisor. Consulte Topologías para implementar el equilibrador de carga de HAProxy.

Le puede resultar útil ver una demostración de cómo se utiliza vSphere with Tanzu con las redes de vDS y HAProxy. Vea el vídeo Introducción al uso de vSphere with Tanzu.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Cree una máquina virtual nueva a partir del archivo OVA de HAProxy.

Opción	Descripción
Biblioteca de contenido	Si importó el archivo OVA a una biblioteca de contenido local: ■ Vaya a **Menú > Biblioteca de contenido**. ■ Seleccione la biblioteca en la que importó el archivo OVA. ■ Seleccione la plantilla `vmware-haproxy-vX.X.X`. ■ Haga clic con el botón derecho y elija **Nueva máquina virtual desde esta plantilla**.
Archivo local	Si descargó el archivo OVA en el host local: ■ Seleccione el clúster de vCenter en el que se habilitará **Administración de cargas de trabajo**. ■ Haga clic con el botón derecho y seleccione **Implementar plantilla de OVF**. ■ Seleccione **Archivo local** y haga clic en **Cargar archivos**. ■ Desplácese hasta el archivo `vmware-haproxy-vX.X.X.ova` y selecciónelo.

3 Introduzca un valor en **Nombre de la máquina virtual**, como **`haproxy`**.

4 Seleccione el **centro de datos** donde va a implementar HAProxy y haga clic en **Siguiente**.

5 Seleccione el clúster de vCenter en el que se habilitará **Administración de cargas de trabajo** y haga clic en **Siguiente**.

6 Revise y confirme los detalles de la implementación y haga clic en **Siguiente**.

7 Acepte los acuerdos de licencia y haga clic en **Siguiente**.

8 Seleccione una configuración de implementación. Consulte Topología de red de HAProxy para obtener detalles.

Configuración	Descripción
Predeterminado	Seleccione esta opción para implementar el dispositivo con 2 NIC: una red de administración y una sola red de cargas de trabajo.
Red de front-end	Seleccione esta opción para implementar el dispositivo con 3 NIC. La subred de front-end se utiliza para aislar los nodos del clúster de la red que utilizan los desarrolladores para acceder al plano de control del clúster.

9 Seleccione la política de almacenamiento que se utilizará para la máquina virtual y haga clic en **Siguiente**.

10 Seleccione las interfaces de red que se utilizarán para el equilibrador de carga y haga clic en **Siguiente**.

Red de origen	Red de destino
Administración	Seleccione la red de administración, como `Red de máquinas virtuales`.
Carga de trabajo	Seleccione el grupo de puertos de vDS configurado para **Administración de cargas de trabajo**.
Front-end	Seleccione el grupo de puertos de vDS configurado para la subred de front-end. Si no seleccionó la configuración de front-end, esta opción se ignorará durante la instalación, por lo que puede dejar el valor predeterminado.

Nota La red de carga de trabajo debe estar en una subred diferente a la red de administración. Consulte los Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y el equilibrador de carga de HAProxy.

11 Personalice los ajustes de configuración de la aplicación. Consulte Ajustes de configuración del dispositivo.

12 Proporcione los detalles de configuración de red. Consulte Configuración de red.

13 Configure el equilibrio de carga. Consulte Configuración del equilibrio de carga.

14 Haga clic en **Siguiente** para completar la configuración del archivo OVA.

15 Revise los detalles de configuración de la implementación y haga clic en **Finalizar** para implementar el archivo OVA.

16 Supervise la implementación de la máquina virtual mediante el panel de **tareas**.

17 Cuando finalice la implementación de la máquina virtual, enciéndala.

Pasos siguientes

Una vez que el equilibrador de carga de HAProxy se implemente y se encienda correctamente, continúe con la habilitación de **Administración de cargas de trabajo**. Consulte Capítulo 5 Configurar y administrar un clúster supervisor.

Personalizar el equilibrador de carga de HAProxy

Personalice la máquina virtual del plano de control de HAProxy, incluidos los ajustes de configuración, la configuración de red y la configuración del equilibrio de carga.

Ajustes de configuración del dispositivo

En la tabla se enumeran y describen los parámetros para configurar el dispositivo de HAProxy.

Parámetro	Descripción	Observación o ejemplo
Contraseña raíz	Contraseña inicial del usuario raíz (6-128 caracteres).	Los cambios subsiguientes de contraseña deben realizarse en el sistema operativo.
Permitir inicio de sesión de usuario raíz	Opción para permitir que el usuario raíz inicie sesión en la máquina virtual de forma remota a través de SSH.	El inicio de sesión de usuario raíz puede ser necesario para solucionar problemas, pero tenga en cuenta las implicaciones de seguridad al conceder este permiso.
Entidad de certificación TLS (ca.crt)	Para utilizar el certificado de CA autofirmado, deje este campo vacío. Para utilizar su propio certificado de CA (ca.crt), pegue su contenido en este campo. Es posible que tenga que codificar el contenido en Base64. https://www.base64encode.org/	Si utiliza el certificado de CA autofirmado, las claves pública y privada se generarán a partir del certificado.
Clave (ca.key)	Si utiliza el certificado autofirmado, deje este campo vacío. Si proporcionó un certificado de CA, pegue el contenido de la clave privada del certificado en este campo.	

Configuración de red

En la tabla se enumeran y describen los parámetros para configurar la red de HAProxy.

Parámetro	Descripción	Observación o ejemplo
Nombre del host	El nombre de host (o FQDN) que se asignará a la máquina virtual del plano de control de HAProxy.	Valor predeterminado: `haproxy.local`
DNS	Una lista separada por comas de direcciones IP del servidor DNS.	Valores predeterminados: `1.1.1.1, 1.0.0.1` Valor de ejemplo: `10.8.8.8`
IP de gestión	La dirección IP estática de la máquina virtual del plano de control de HAProxy en la red de administración.	Una dirección IPv4 válida con la longitud de prefijo de la red; por ejemplo: `192.168.0.2/24`.
Puerta de enlace de administración	La dirección IP de la puerta de enlace para la red de administración.	Por ejemplo: `192.168.0.1`
IP de carga de trabajo	La dirección IP estática de la máquina virtual del plano de control de HAProxy en la red de cargas de trabajo. Esta dirección IP debe estar fuera del rango de direcciones IP del equilibrador de carga.	Una dirección IPv4 válida con la longitud de prefijo de la red; por ejemplo: `192.168.10.2/24`.
Puerta de enlace de carga de trabajo	La dirección IP de la puerta de enlace para la red de cargas de trabajo.	Por ejemplo: `192.168.10.1` Si selecciona la configuración de front-end, debe introducir una puerta de enlace. La implementación no se realizará correctamente si se selecciona el front-end y no se especifica ninguna puerta de enlace.
IP de front-end	La dirección IP estática del dispositivo de HAProxy en la red de front-end. Este valor solo se utiliza cuando se selecciona el modelo de implementación de front-end.	Una dirección IPv4 válida con la longitud de prefijo de la red; por ejemplo: `192.168.100.2/24`
Puerta de enlace de front-end	La dirección IP de la puerta de enlace para la red de front-end. Este valor solo se utiliza cuando se selecciona el modelo de implementación de front-end.	Por ejemplo: `192.168.100.1`

Configuración del equilibrio de carga

En la tabla se enumeran y describen los parámetros para configurar el equilibrador de carga de HAProxy.

Parámetro	Descripción	Ejemplo u observación
Rango(s) de direcciones IP del equilibrador de carga	En este campo se especifica un rango de direcciones IPv4 con el formato CIDR. El valor debe ser un rango de CIDR válido o se producirá un error en la instalación. HAProxy reserva las direcciones IP para las direcciones IP virtuales (VIP). Una vez se asignan, se asignará cada dirección VIP, HAProxy responderá a las solicitudes de esa dirección. El rango de CIDR que se especifique aquí no deberá superponerse con las direcciones IP que se asignen para los servidores virtuales cuando se habilite **Administración de cargas de trabajo** en vCenter Server mediante vSphere Client.	Por ejemplo, el CIDR de red `192.168.100.0/24` proporciona las 256 direcciones IP virtuales del equilibrador de carga con el rango `192.168.100.0 - 192.168.100.255`. Por ejemplo, el CIDR de red `192.168.100.0/25` proporciona las 128 direcciones IP virtuales del equilibrador de carga con el rango `192.168.100.0 - 192.168.100.127`.
Puerto de administración de la API del plano de datos	El puerto de la máquina virtual de HAProxy en el que escucha el servicio de API del equilibrador de carga.	Un puerto válido. El puerto 22 se reserva para SSH. El valor predeterminado es `5556`.
ID de usuario de HAProxy	Nombre de usuario de la API del equilibrador de carga	El nombre de usuario que utilizan los clientes para autenticarse en el servicio de API del equilibrador de carga. **Nota** Necesita este nombre de usuario cuando habilite clúster supervisor.
Contraseña de HAProxy	Contraseña de la API del equilibrador de carga	La contraseña que utilizan los clientes para autenticarse en el servicio de API del equilibrador de carga. **Nota** Necesita esta contraseña cuando habilite el clúster supervisor.

Configurar y administrar un clúster supervisor

5

Como administrador de vSphere, habilite un clúster de vSphere para Administración de cargas de trabajo mediante la creación de un clúster supervisor. Puede seleccionar entre crear el clúster supervisor con la pila de redes de vSphere o con NSX-T Data Center como solución de red. Un clúster configurado con NSX-T Data Center admite la ejecución de un pod de vSphere y un clúster de Tanzu Kubernetes que se hayan creado a través de servicio VMware Tanzu™ Kubernetes Grid™. Una instancia de clúster supervisor que se configura con la pila de redes de vSphere solo admite clústeres de Tanzu Kubernetes.

Después de habilitar el clúster supervisor, puede utilizar vSphere Client para administrar y supervisar el clúster.

Este capítulo incluye los siguientes temas:

- Requisitos previos para configurar vSphere with Tanzu en un clúster de vSphere
- Habilitar la administración de cargas de trabajo con redes de vSphere
- Habilitar la administración de cargas de trabajo con redes de NSX-T Data Center
- Asignar la licencia de Tanzu Edition a clúster supervisor
- Reemplazar el certificado VIP para conectarse de forma segura al endpoint de API de clúster supervisor
- Integrar servicio Tanzu Kubernetes Grid en el clúster supervisor con Tanzu Mission Control
- Configurar la CNI predeterminada para los clústeres de Tanzu Kubernetes
- Agregar redes de cargas de trabajo a un clúster supervisor configurada con redes de VDS
- Cambiar el tamaño del plano de control de un clúster supervisor
- Cambiar la configuración de red de administración en un clúster supervisor
- Cambiar la configuración de red de carga de trabajo en un clúster supervisor configurada con redes de VDS
- Cambiar la configuración de red de carga de trabajo en un clúster supervisor configurada con NSX-T Data Center
- Resolución de estados de errores en clúster supervisor durante la configuración inicial o la actualización
- Configuración de los ajustes del proxy HTTP en vSphere with Tanzu

- Transmitir registros del plano de control de clúster supervisor a un rsyslog remoto

Requisitos previos para configurar vSphere with Tanzu en un clúster de vSphere

Compruebe los requisitos previos para habilitar vSphere with Tanzu en su entorno de vSphere. Para ejecutar cargas de trabajo basadas en contenedores de forma nativa en vSphere como administrador de vSphere, habilite **Administración de cargas de trabajo** en un clúster de vSphere. El resultado es un clúster de administración de Kubernetes conocido como clúster supervisor donde se ejecutan pods de vSphere y se aprovisionan clústeres de Tanzu Kubernetes.

Crear y configurar un clúster de vSphere

Un clúster de vSphere es una recopilación de hosts ESXi administrados por un sistema vCenter Server. El clúster supervisor se ejecuta en un clúster de vSphere. Cree un clúster de vSphere que cumpla con los siguientes requisitos para poder habilitar **Administración de cargas de trabajo** en él:

- Cree y configure un clúster de vSphere con al menos tres hosts ESXi. Si utiliza vSAN, se recomienda utilizar cuatro hosts ESXi, pero no es necesario. Consulte Crear y configurar clústeres.
- Configure el clúster con almacenamiento compartido, como vSAN. Se requiere almacenamiento compartido para vSphere HA, DRS y para almacenar volúmenes contenedores persistentes. Consulte Crear un clúster de vSAN .
- Si tiene pensado utilizar volúmenes persistentes en modo ReadWriteMany, habilite los servicios de archivos en el clúster de vSAN. Consulte Crear volúmenes persistentes ReadWriteMany en vSphere with Tanzu.
- Habilite el clúster con vSphere HA. Consulte Crear y usar clústeres de vSphere HA.
- Habilite el clúster con vSphere DRS en modo totalmente automatizado. Consulte Crear un clúster de DRS.
- Compruebe que la cuenta de usuario tenga **Modificar configuración de todo el clúster** en el clúster de vSphere para poder habilitar la funcionalidad **Administración de cargas de trabajo**.

Precaución No deshabilite vSphere DRS después de configurar el clúster supervisor. Tener DRS habilitado en todo momento es un requisito previo obligatorio para ejecutar cargas de trabajo en el clúster supervisor. Si se deshabilita DRS, se interrumpirán los clústeres de Tanzu Kubernetes.

Elegir y configurar la pila de redes

Para habilitar **Administración de cargas de trabajo** en un clúster de vSphere, debe configurar la pila de redes que se utilizarán en clúster supervisor. Dispone de dos opciones: NSX-T Data Center o redes de vSphere Distributed Switch (vDS) con un equilibrador de carga. Puede configurar el NSX Advanced Load Balancer o el equilibrador de carga de HAProxy.

En la tabla se enumeran las diferencias de alto nivel entre las dos pilas de redes admitidas. Para obtener más información sobre las diferencias en arquitectura, consulte clúster supervisor configurado con la pila de redes de vSphere.

Funcionalidad	Redes de NSX-T	Redes de vDS
pods de vSphere	Sí	No
Tanzu Kubernetes clústeres	Sí	Sí
Instancia de registro de Harbor integrada	Sí	No
Equilibrio de carga	Sí	Sí, mediante la instalación y configuración de NSX Advanced Load Balancer o el equilibrador de carga de HAProxy.

Para usar las redes de NSX-T Data Center para el clúster supervisor:

- Revise los requisitos del sistema y las topologías para redes de NSX-T. Consulte Requisitos del sistema para configurar vSphere with Tanzu con NSX-T Data Center.
- Instale y configure NSX-T Data Center para vSphere with Tanzu. Consulte Instalar y configurar NSX-T Data Center para vSphere with Tanzu.

Para utilizar redes de vSphere vDS con el NSX Advanced Load Balancer para el clúster supervisor:

- Revise los requisitos de NSX Advanced Load Balancer. Consulte Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y NSX Advanced Load Balancer.
- Cree una instancia de vSphere Distributed Switch (vDS), agregue todos los hosts ESXi del clúster a vDS y cree grupos de puertos para las redes de cargas de trabajo. Consulte Crear una instancia de vSphere Distributed Switch para un clúster supervisor para su uso con NSX Advanced Load Balancer.
- Implemente y configure el NSX Advanced Load Balancer. Consulte Implementar el controlador.

Nota vSphere with Tanzu admite NSX Advanced Load Balancer con vSphere 7 U2 y versiones posteriores.

Para utilizar redes de vSphere vDS con el equilibrio de carga de HAProxy para el clúster supervisor:

- Revise los requisitos del sistema y las topologías de red para redes de vSphere con un equilibrador de carga externo. Consulte Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y el equilibrador de carga de HAProxy y Topologías para implementar el equilibrador de carga de HAProxy.
- Cree una instancia de vSphere Distributed Switch (vDS), agregue todos los hosts ESXi del clúster a vDS y cree grupos de puertos para las redes de cargas de trabajo. Consulte Crear una instancia de vSphere Distributed Switch para un clúster supervisor para su uso con el equilibrador de carga de HAProxy.

- Instale y configure un equilibrador de carga de HAProxy que se pueda enrutar a la instancia de vSphere Distributed Switch que está conectada a los hosts desde el clúster de vSphere. El equilibrador de carga de HAProxy admite la conectividad de red con las cargas de trabajo de las redes de clientes y para equilibrar la carga del tráfico entre los clústeres de Tanzu Kubernetes. Consulte Instalar y configurar el equilibrador de carga de HAProxy.

Nota vSphere with Tanzu admite el equilibrador de carga de HAProxy con vSphere 7 U1 y versiones posteriores.

Crear directiva de almacenamiento

Debe crear directivas de almacenamiento que determinen la ubicación del almacén de datos de las máquinas virtuales, los contenedores y las imágenes del plano de control de Kubernetes. Puede crear directivas de almacenamiento que se asocien con diferentes clases de almacenamiento.

Antes de habilitar **Administración de cargas de trabajo** en un clúster de vSphere, cree una directiva de almacenamiento para la colocación de máquinas virtuales del plano de control de Kubernetes. Consulte Crear directivas de almacenamiento para vSphere with Tanzu.

Crear una biblioteca de contenido

Para aprovisionar clústeres de Tanzu Kubernetes, se necesita una **biblioteca de contenido** que se cree en la instancia de vCenter Server que administra el clúster de vSphere en el que se ejecuta el clúster supervisor.

La **biblioteca de contenido** proporciona el sistema con las distribuciones de las versiones de Tanzu Kubernetes en forma de plantillas de OVA. Al aprovisionar un clúster de Tanzu Kubernetes, la plantilla de OVA de la versión seleccionada se utiliza para crear los nodos del clúster de Kubernetes.

Puede crear una **biblioteca de contenido suscrita** para extraer automáticamente las últimas imágenes publicadas o bien puede crear una **biblioteca de contenido local** y cargar manualmente las imágenes, que se pueden necesitar para el aprovisionamiento aislado de clústeres de Tanzu Kubernetes.

Consulte Crear y administrar bibliotecas de contenido para versiones de Tanzu Kubernetes.

Ver demostraciones de vSphere with Tanzu

Si bien no es un requisito estricto, antes de comenzar, puede resultar útil ver algunas demostraciones de vSphere with Tanzu, como la configuración del entorno de vSphere para preparar la implementación del clúster supervisor, la habilitación de **Administración de cargas de trabajo** y el aprovisionamiento de los clústeres de Tanzu Kubernetes. Si lo encuentra útil, consulte la serie de vídeos de información detallada de vSphere with Tanzu en el canal de Vmware vSphere. También puede revisar la serie de vídeos cortos Bytes rápidos de vSphere Tanzu para configurar **Administración de cargas de trabajo** con las redes de vDS y el equilibrador de cargas de HAProxy.

Habilitar la administración de cargas de trabajo con redes de vSphere

Como administrador de vSphere, puede habilitar la plataforma **Administración de cargas de trabajo** en un clúster de vSphere mediante la configuración de la pila de redes de vSphere para proporcionar conectividad a las cargas de trabajo. Una instancia de clúster supervisor que se configura con redes de vSphere es compatible con la implementación de clústeres de Tanzu Kubernetes creados mediante el servicio Tanzu Kubernetes Grid. No admite la ejecución de pod de vSphere o el uso del registro de Harbor integrado.

Precaución No deshabilite vSphere DRS después de configurar el clúster supervisor. Tener DRS habilitado en todo momento es un requisito previo obligatorio para ejecutar cargas de trabajo en el clúster supervisor. Si se deshabilita DRS, se interrumpirán los clústeres de Tanzu Kubernetes.

Requisitos previos

- Complete los requisitos previos para configurar un clúster de vSphere como un clúster supervisor. Consulte Requisitos previos para configurar vSphere with Tanzu en un clúster de vSphere.

Procedimiento

1 En el menú de inicio, seleccione **Administración de cargas de trabajo**.

2 Seleccione una opción de licencias para clúster supervisor.

   - Si tiene una licencia de Tanzu Edition válida, haga clic en **Agregar licencia** para agregar la clave de licencia al inventario de licencias de vSphere.
   - Si aún no tiene una licencia de Tanzu Edition, introduzca los detalles de contacto para poder recibir la comunicación de VMware y haga clic en **Comenzar**.

   El período de evaluación de clúster supervisor dura 60 días. Dentro de ese período, debe asignar una licencia válida de Tanzu Edition al clúster. Si agregó una clave de licencia de Tanzu Edition, podrá asignar esa misma clave en el período de evaluación de 60 días una vez que haya completado la configuración de clúster supervisor.

3 En la pantalla **Administración de cargas de trabajo**, haga clic de nuevo en **Comenzar**.

4 Seleccione un sistema de vCenter Server, seleccione **Red de vCenter Server** y haga clic en **Siguiente**.

5 Seleccione un clúster de la lista de destinos compatibles.

6 En la página **Tamaño del plano de control**, seleccione el tamaño de las máquinas virtuales del plano de control de Kubernetes que se crearán en cada host del clúster.

   La cantidad de recursos que se asignan a las máquinas virtuales del plano de control determina la cantidad de cargas de trabajo de Kubernetes que podrá administrar el clúster supervisor.

7 En la pantalla **Equilibrador de carga**, seleccione el equilibrador de carga que desea utilizar. Puede seleccionar NSX Advanced Load Balancer o HAProxy.

- Introduzca la siguiente configuración para NSX Advanced Load Balancer:

Opción	Descripción
Nombre	Introduzca un nombre para NSX Advanced Load Balancer.
IP del controlador de AVI	Dirección IP del controlador de NSX Advanced Load Balancer. El puerto predeterminado es `443`.
Nombre de usuario	El nombre de usuario que está configurado con NSX Advanced Load Balancer. Utilice este nombre de usuario para acceder al controlador.
Contraseña	La contraseña para el nombre de usuario.
Entidad de certificación de servidor	El certificado utilizado por el controlador. Puede proporcionar el certificado que asignó durante la configuración. Para obtener más información, consulte Asignar un certificado al controlador.

- Introduzca la siguiente configuración para HAProxy:

Opción	Descripción
Nombre	Un nombre descriptivo para el equilibrador de carga.
Direcciones de API del plano de datos	La dirección IP y el puerto de la API del plano de datos de HAProxy. Este componente controla el servidor de HAProxy y se ejecuta dentro de la máquina virtual de HAProxy. Esta es la dirección IP de la red de administración del dispositivo de HAProxy.
Nombre de usuario	El nombre de usuario que está configurado con el archivo OVA de HAProxy. Este nombre se utiliza para autenticarse con la API del plano de datos de HAProxy.
Contraseña	La contraseña para el nombre de usuario.

Opción	Descripción
Rangos de direcciones IP para servidores virtuales	Rango de direcciones IP que utilizan los clústeres de Tanzu Kubernetes en la red de cargas de trabajo. Este rango de IP proviene de la lista de direcciones IP que se definieron en el CIDR que configuró durante la implementación del dispositivo de HAProxy. Por lo general, este será el rango completo especificado en la implementación de HAProxy, pero también puede ser un subconjunto de ese CIDR, ya que puede crear varios clústeres supervisor y utilizar direcciones IP de ese rango de CIDR. Este rango no debe superponerse con el rango de IP definido para la red de cargas de trabajo en este asistente. El rango tampoco debe superponerse con ningún ámbito DHCP en esta red de cargas de trabajo.
Entidad de certificación de servidor	El certificado en formato PEM que está firmado o es una raíz de confianza del certificado de servidor que presenta la API del plano de datos. ■ Opción 1: Si se habilita el acceso raíz, ejecute SSH en la máquina virtual de HAProxy como usuario raíz y copie `/etc/haproxy/ca.crt` en la **Entidad de certificación de servidor**. No utilice líneas de escape con el formato `\n`. ■ Opción 2: Haga clic con el botón derecho en la máquina virtual de HAProxy y seleccione **Editar configuración**. Copie el certificado de CA desde el campo correspondiente y conviértalo desde Base64 mediante una herramienta de conversión como https://www.base64decode.org/. ■ Opción 3: Ejecute el siguiente script de PowerCLI. Reemplace las variables `$vc`, `$vc_user` y `$vc_password` con los valores correspondientes. `$vc = "10.21.32.43"` `$vc_user =` `"administrator@vsphere.local"` `$vc_password = "PASSWORD"` `Connect-VIServer -User $vc_user` `-Password $vc_password -Server $vc` `$VMname = "haproxy-demo"` `$AdvancedSettingName =` `"guestinfo.dataplaneapi.cacert"` `$Base64cert = get-vm $VMname \|Get-` `AdvancedSetting -Name` `$AdvancedSettingName` `while` `([string]::IsNullOrEmpty($Base64cert.V` `alue)) {` `     Write-Host "Waiting for CA Cert` `Generation... This may take a under` `5-10` `minutes as the VM needs to boot and` `generate the CA Cert` `(if you haven't provided one` `already)."`

Opción	Descripción
	`` $Base64cert = get-vm $VMname | Get-AdvancedSetting -Name $AdvancedSettingName Start-sleep -seconds 2 } Write-Host "CA Cert Found... Converting from BASE64" $cert = [Text.Encoding]::Utf8.GetString([Conve rt]::FromBase64String($Base64cert.Valu e)) Write-Host $cert ```

8 En la pantalla **Red de administración**, configure los parámetros de la red que se utilizarán para las máquinas virtuales del plano de control de Kubernetes.

a Seleccione un **Modo de red**.

- **Red DHCP**. En este modo, todas las direcciones IP de la red de administración, como las direcciones IP de las máquinas virtuales del plano de control, una dirección IP flotante, los servidores DNS, DNS, los dominios de búsqueda y el servidor NTP, se adquieren automáticamente desde un servidor DHCP. Para obtener direcciones IP flotantes, el servidor DHCP debe estar configurado para admitir identificadores de cliente. En el modo DHCP, todas las máquinas virtuales del plano de control utilizan identificadores de cliente DHCP estables para adquirir direcciones IP. Estos identificadores de cliente se pueden utilizar para configurar la asignación de direcciones IP estáticas para que las direcciones IP de las máquinas virtuales del plano de control en el servidor DHCP se aseguren de que no cambien. No se admite el cambio de las direcciones IP de las máquinas virtuales del plano de control, así como las direcciones IP flotantes.
- **Estático**. Introduzca manualmente toda la configuración de red de la red de administración.

b Configure los parámetros de la red de administración.

Si seleccionó el modo de red DHCP, pero desea anular la configuración adquirida en el DHCP, haga clic en **Configuración adicional** e introduzca nuevos valores. Si seleccionó el modo de red estática, rellene manualmente los valores de configuración de la red de administración.

Opción	Descripción
Red	Seleccione una red que tenga un adaptador de VMkernel configurado para el tráfico de administración.
Iniciar la dirección IP de control	Introduzca una dirección IP que determine el punto de inicio para reservar cinco direcciones IP consecutivas para las máquinas virtuales del plano de control de Kubernetes de la siguiente manera: ■ Una dirección IP para cada una de las máquinas virtuales del plano de control de Kubernetes. ■ Una dirección IP flotante para una de las máquinas virtuales del plano de control de Kubernetes a la que se prestará servicio como una interfaz a la red de administración. La máquina virtual del plano de control que tiene asignada la dirección IP flotante actúa como una máquina virtual principal para las tres máquinas virtuales del plano de control de Kubernetes. La dirección IP flotante se traslada al nodo del plano de control que es el líder de ectd en el clúster de Kubernetes. Esto mejora la disponibilidad en el caso de un evento de partición de red. ■ Una dirección IP que se va a utilizar como búfer en caso de que una máquina virtual de plano de control de Kubernetes falle y se ponga en marcha una nueva máquina virtual de plano de control para reemplazarla.

Opción	Descripción
Máscara de subred	Solo se aplica a la configuración de IP estática. Introduzca una máscara de subred para la red de administración. Por ejemplo, `255.255.255.0`
Servidores DNS	Introduzca las direcciones de los servidores DNS que utiliza en su entorno. Si el sistema vCenter Server está registrado con un FQDN, debe introducir las direcciones IP de los servidores DNS que utiliza con el entorno de vSphere para que el FQDN se pueda resolver en el clúster supervisor.
Dominios de búsqueda DNS	Introduzca los nombres de dominio que DNS busca dentro de los nodos del plano de control de Kubernetes, como `corp.local`, para que el servidor DNS pueda resolverlos.
NTP	Introduzca las direcciones de los servidores NTP que utiliza en su entorno, si los hubiera.

9 En la página **Red de carga de trabajo**, introduzca la configuración de la red que controlará el tráfico de red de las cargas de trabajo de Kubernetes que se ejecutan en clúster supervisor.

Nota Si selecciona el uso de un servidor DHCP para proporcionar la configuración de red para las redes de carga de trabajo, no podrá crear ninguna red de carga de trabajo nueva una vez que complete la configuración del clúster supervisor.

a Seleccione un modo de red.

- **Red DHCP**. En este modo de red, toda la configuración de red de las redes de carga de trabajo se adquiere a través de DHCP.
- **Estático**. Configure manualmente los ajustes de la red de carga de trabajo.

b Seleccione el grupo de puertos que servirá como red de carga de trabajo principal en el clúster supervisor.

La red principal controla el tráfico de las máquinas virtuales del plano de control de Kubernetes y el tráfico de las cargas de trabajo de Kubernetes.

En función de la topología de red, podrá asignar más adelante un grupo de puertos diferente que sirva como red para cada espacio de nombres. De esta forma, podrá proporcionar aislamiento de capa 2 entre los espacios de nombres en clúster supervisor. Los espacios de nombres que no tienen un grupo de puertos diferente asignado como red usan la red principal. Los clústeres de Tanzu Kubernetes solo usan la red que está asignada al espacio de nombres en el que se implementan o bien utilizan la red principal si no hay ninguna red explícita asignada a ese espacio de nombres.

c Configure los ajustes de las redes de carga de trabajo.

Si seleccionó el modo de red DHCP, todos los valores de la sección **Configuración adicional** se rellenan automáticamente a partir del servidor DHCP. Si desea anular estos valores, haga clic en **Configuración adicional** e introduzca nuevos valores. Si seleccionó el modo de red **Estático**, rellene todos los ajustes manualmente.

Opción	Descripción
Red interna para servicios de Kubernetes	Introduzca una anotación de CIDR que determine el rango de direcciones IP para los clústeres y los servicios de Tanzu Kubernetes que se ejecutan dentro de los clústeres.
Nombre de red	Introduzca el nombre de la red.
servidor DNS	Introduzca las direcciones IP de los servidores DNS que utiliza con su entorno, si los hubiera. Por ejemplo, `10.142.7.1`. Cuando se introduce la dirección IP del servidor DNS, se agrega una ruta estática a cada máquina virtual del plano de control. Esto indica que el tráfico a los servidores DNS pasa por la red de cargas de trabajo. Si los servidores DNS que especifica se comparten entre la red de administración y la red de cargas de trabajo, las búsquedas de DNS en las máquinas virtuales del plano de control se enrutan a través de la red de cargas de trabajo después de la configuración inicial.

Opción	Descripción
Puerta de enlace	Introduzca la puerta de enlace de la red principal.
IP de máscara de subred	Introduzca la dirección IP de la máscara de subred.
Rangos de direcciones IP	Introduzca un rango de direcciones IP para asignar la dirección IP de las máquinas virtuales y las cargas de trabajo del plano de control de Kubernetes. Este rango de direcciones conecta los nodos del clúster supervisor y, en el caso de una sola red de cargas de trabajo, también conecta los nodos del clúster de Tanzu Kubernetes. Este rango de direcciones IP no debe superponerse con el rango de VIP del equilibrador de carga cuando se utiliza la configuración **Predeterminado** para HAProxy.

10 En la página **Almacenamiento**, configure la compatibilidad con el almacenamiento y el volumen de archivos.

a Seleccione directivas de almacenamiento para el clúster supervisor.

La directiva de almacenamiento que seleccione para cada uno de los siguientes objetos garantiza que el objeto se coloque en el almacén de datos al que se hace referencia en la directiva de almacenamiento. Puede utilizar directivas de almacenamiento iguales o diferentes para los objetos.

Opción	Descripción
Nodo del plano de control	Seleccione la directiva de almacenamiento para la colocación de las máquinas virtuales del plano de control.
Discos efímeros del pod	Seleccione la directiva de almacenamiento para la colocación de los pods de vSphere.
Memoria caché de imágenes de contenedor	Seleccione la directiva de almacenamiento para la colocación de la memoria caché de las imágenes de contenedor.

b (opcional) Active la compatibilidad con volúmenes de archivos.

Esta opción es necesaria si planea implementar volúmenes persistentes ReadWriteMany en un clúster. Consulte Crear volúmenes persistentes ReadWriteMany en vSphere with Tanzu.

11 En la página **Tanzu Kubernetes Grid**, haga clic en **Agregar** y seleccione la biblioteca de contenido suscrita que contiene las imágenes de máquinas virtuales que se utilizan para implementar los nodos de los clústeres de Tanzu Kubernetes.

12 Repase la configuración y haga clic en **Finalizar**.

Resultados

Se ejecuta una tarea en vCenter Server que crea el clúster supervisor. Una vez finalizada la tarea, se crean tres máquinas virtuales del plano de control de Kubernetes en los hosts que formen parte del clúster de vSphere.

Pasos siguientes

Cree y configure espacios de nombres de vSphere en el clúster supervisor. Consulte Creación y configuración de un espacio de nombres de vSphere.

Habilitar la administración de cargas de trabajo con redes de NSX-T Data Center

Como administrador de vSphere, puede configurar un clúster de vSphere como una instancia de clúster supervisor que utilice la pila de redes de NSX-T Data Center para proporcionar conectividad a las cargas de trabajo de Kubernetes.

Requisitos previos

- Compruebe que el entorno cumpla con los requisitos previos para configurar un clúster de vSphere como un clúster supervisor. Para obtener información sobre los requisitos, consulte Requisitos previos para configurar vSphere with Tanzu en un clúster de vSphere.

Precaución No deshabilite vSphere DRS después de configurar el clúster supervisor. Tener DRS habilitado en todo momento es un requisito previo obligatorio para ejecutar cargas de trabajo en el clúster supervisor. Si se deshabilita DRS, se interrumpirán los clústeres de Tanzu Kubernetes.

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Haga clic en **Comenzar**.

3 Seleccione el sistema de vCenter Server que desea configurar.

4 Seleccione la pila de redes de **NSX**.

5 Haga clic en **Siguiente**.

6 Seleccione **Seleccionar un clúster > Centro de datos**.

7 Seleccione un clúster de la lista de clústeres compatibles y haga clic en **Siguiente**.

8 En la página **Tamaño del plano de control**, seleccione el tamaño de las máquinas virtuales del plano de control.

   El tamaño de las máquinas virtuales del plano de control determina la cantidad de cargas de trabajo que puede ejecutar en clúster supervisor.

   Para obtener instrucciones, consulte el sitio Valores máximos de configuración de VMware.

9 Haga clic en **Siguiente**.

10 En la pantalla **Red de administración**, configure los parámetros de la red que se utilizarán para las máquinas virtuales del plano de control de Kubernetes.

a Seleccione un **Modo de red**.

- **Red DHCP**. En este modo, todas las direcciones IP de la red de administración, como las direcciones IP de las máquinas virtuales del plano de control, los servidores DNS, DNS, los dominios de búsqueda y el servidor NTP, se adquieren automáticamente desde un servidor DHCP.
- **Estático**. Introduzca manualmente toda la configuración de red de la red de administración.

b Configure los parámetros de la red de administración.

Si seleccionó el modo de red DHCP, pero desea anular la configuración adquirida en el DHCP, haga clic en **Configuración adicional** e introduzca nuevos valores. Si seleccionó el modo de red estática, rellene manualmente los valores de configuración de la red de administración.

Opción	Descripción
Red	Seleccione una red que tenga un adaptador de VMkernel configurado para el tráfico de administración.
Iniciar la dirección IP de control	Introduzca una dirección IP que determine el punto de inicio para reservar cinco direcciones IP consecutivas para las máquinas virtuales del plano de control de Kubernetes de la siguiente manera: ■ Una dirección IP para cada una de las máquinas virtuales del plano de control de Kubernetes. ■ Una dirección IP flotante para una de las máquinas virtuales del plano de control de Kubernetes a la que se prestará servicio como una interfaz a la red de administración. La máquina virtual del plano de control que tiene asignada la dirección IP flotante actúa como una máquina virtual principal para las tres máquinas virtuales del plano de control de Kubernetes. La dirección IP flotante se traslada al nodo del plano de control que es el líder de ectd en este clúster de Kubernetes, que es el clúster supervisor. Esto mejora la disponibilidad en el caso de un evento de partición de red. ■ Una dirección IP que se va a utilizar como búfer en caso de que una máquina virtual de plano de control de Kubernetes falle y se ponga en marcha una nueva máquina virtual de plano de control para reemplazarla.
Máscara de subred	Solo se aplica a la configuración de IP estática. Introduzca una máscara de subred para la red de administración. Por ejemplo, `255.255.255.0`
Servidores DNS	Introduzca las direcciones de los servidores DNS que utiliza en su entorno. Si el sistema vCenter Server está registrado con un FQDN, debe introducir las direcciones IP de los servidores DNS que utiliza con el entorno de vSphere para que el FQDN se pueda resolver en el clúster supervisor.

Opción	Descripción
Dominios de búsqueda DNS	Introduzca los nombres de dominio que DNS busca dentro de los nodos del plano de control de Kubernetes, como `corp.local`, para que el servidor DNS pueda resolverlos.
NTP	Introduzca las direcciones de los servidores NTP que utiliza en su entorno, si los hubiera.

11 En el panel **Red de cargas de trabajo**, configure las opciones de las redes para los espacios de nombres.

La configuración de red del espacio de nombres proporciona conectividad con los pods de vSphere y los espacios de nombres que se ejecutan en el clúster supervisor. De forma predeterminada, el espacio de nombres utilizará la configuración de red en el nivel de clúster.

Opción	Descripción
vSphere Distributed Switch	Seleccione la instancia de vSphere Distributed Switch que controla las redes de superposición para clúster supervisor. Por ejemplo, seleccione `DSwitch`.
servidor DNS	Introduzca las direcciones IP de los servidores DNS que utiliza con su entorno, si los hubiera. Por ejemplo, `10.142.7.1`.
FQDN de endpoint de servidor de API	De forma opcional, introduzca el FQDN del endpoint del servidor de API.
Clúster de Edge	Seleccione el clúster de NSX Edge que tenga la puerta de enlace de nivel 0 que desee utilizar para las redes de espacio de nombres. Por ejemplo, seleccione `EDGE-CLUSTER`.
Puerta de enlace de nivel 0	Seleccione la puerta de enlace de nivel 0 que se asociará con la puerta de enlace de nivel 1 del clúster.
Modo NAT	El modo NAT está seleccionado de forma predeterminada. Si anula la selección de la opción, se podrá acceder directamente a todas las cargas de trabajo, como los pods de vSphere, las máquinas virtuales y las direcciones IP de los nodos de los clústeres de Tanzu Kubernetes desde fuera de la puerta de enlace de nivel 0, y no tendrá que configurar los CIDR de salida. **Nota** Si anula la selección del modo NAT, no se admitirá el almacenamiento de volumen de archivos.
Red de espacio de nombres	Introduzca uno o varios CIDR de IP para crear subredes o segmentos y asignar direcciones IP a las cargas de trabajo.
Prefijo de subred de espacio de nombres	Introduzca el prefijo de subred que especifica el tamaño de la subred reservada para los segmentos de espacios de nombres. El valor predeterminado es 28.
CIDR del pod	Introduzca una anotación CIDR para determinar el rango de IP de los pods nativos de vSphere. Puede utilizar el valor predeterminado.
CIDR de servicios	Introduzca una anotación CIDR para determinar el rango de IP de los servicios de Kubernetes. Puede utilizar el valor predeterminado.

Opción	Descripción
CIDR de entrada	Introduzca una anotación CIDR que determine el rango de IP de entrada para los servicios de Kubernetes. Este rango se utiliza para los servicios de tipo equilibrador de carga y entrada.
CIDR de egreso	Introduzca una anotación CIDR que determine la IP de salida de los servicios de Kubernetes. Solo se asigna una dirección IP de egreso para cada espacio de nombres en el clúster supervisor. La IP de salida es la dirección IP que los pods de vSphere en el espacio de nombres concreto usa para comunicarse fuera de NSX-T Data Center.

12 Haga clic en **Siguiente**.

13 En la página **Almacenamiento**, configure la compatibilidad con el almacenamiento y el volumen de archivos.

a Seleccione directivas de almacenamiento para el clúster supervisor.

La directiva de almacenamiento que seleccione para cada uno de los siguientes objetos garantiza que el objeto se coloque en el almacén de datos al que se hace referencia en la directiva de almacenamiento. Puede utilizar directivas de almacenamiento iguales o diferentes para los objetos.

Opción	Descripción
Nodo del plano de control	Seleccione la directiva de almacenamiento para la colocación de las máquinas virtuales del plano de control.
Discos efímeros del pod	Seleccione la directiva de almacenamiento para la colocación de los pods de vSphere.
Memoria caché de imágenes de contenedor	Seleccione la directiva de almacenamiento para la colocación de la memoria caché de las imágenes de contenedor.

b (opcional) Active la compatibilidad con volúmenes de archivos.

Esta opción es necesaria si planea implementar volúmenes persistentes ReadWriteMany en un clúster. Consulte Crear volúmenes persistentes ReadWriteMany en vSphere with Tanzu.

14 En la sección **Listo para finalizar**, revise la configuración y haga clic en **Finalizar**.

El clúster se habilita con la vSphere with Tanzu y se pueden crear espacios de nombres de vSphere para proporcionarlos a los ingenieros de desarrollo y operaciones. Se crean nodos de plano de control de Kubernetes en los hosts que forman parte del clúster y del proceso de Spherelet.

Pasos siguientes

Cree y configure un espacio de nombres de vSphere en el clúster supervisor. Consulte Creación y configuración de un espacio de nombres de vSphere.

Asignar la licencia de Tanzu Edition a clúster supervisor

Si utiliza clúster supervisor en modo de evaluación, debe asignar una licencia de Tanzu Edition al clúster antes de que finalice el período de evaluación de 60 días.

Consulte Licencias para vSphere with Tanzu para obtener información sobre cómo funciona la licencia de Tanzu.

Procedimiento

1 En vSphere Client, desplácese hasta clúster supervisor.

2 Seleccione **Configurar** y, en **Licencias**, seleccione **Supervisor Cluster**.

3 Seleccione **Asignar licencia**.

4 En el cuadro de diálogo **Asignar licencia**, haga clic en **Nueva licencia**.

5 Introduzca una clave de licencia válida y haga clic en **Aceptar**.

Reemplazar el certificado VIP para conectarse de forma segura al endpoint de API de clúster supervisor

Como administrador de vSphere, puede reemplazar el certificado de la dirección IP virtual (virtual IP address, VIP) para conectarse de forma segura al endpoint de API de clúster supervisor con un certificado firmado por una CA en la que los hosts ya confíen. El certificado autentica el plano de control de Kubernetes para los ingenieros de desarrollo y operaciones, tanto en el inicio de sesión como en las interacciones posteriores con el clúster supervisor.

Requisitos previos

Compruebe que puede acceder a una CA que pueda firmar CSR. Para los ingenieros de desarrollo y operaciones, la CA debe estar instalada en su sistema como una raíz de confianza.

Procedimiento

1 En vSphere Client, desplácese hasta clúster supervisor.

2 Haga clic en **Configurar**; a continuación, en **Espacios de nombres**, seleccione **Certificados**.

3 En el panel **MTG de la plataforma de carga de trabajo**, seleccione **Acciones > Generar CSR**.

4 Proporcione los detalles del certificado.

5 Una vez que se genere la CSR, haga clic en **Copiar**.

6 Firme el certificado con una CA.

7 En el panel **MTG de la plataforma de carga de trabajo**, seleccione **Acciones > Reemplazar certificado**.

8 Cargue el archivo de certificado firmado y haga clic en **Reemplazar certificado**.

9 Valide el certificado en la dirección IP del plano de control de Kubernetes.

Por ejemplo, puede abrir la página de descarga de Herramientas de la CLI de Kubernetes para vSphere y confirmar que el certificado fue reemplazado correctamente desde el navegador. En un sistema Linux o Unix, también puede utilizar `echo | openssl s_client -connect https://ip:6443`.

Integrar servicio Tanzu Kubernetes Grid en el clúster supervisor con Tanzu Mission Control

La instancia de servicio Tanzu Kubernetes Grid que se ejecuta en el clúster supervisor se puede integrar con Tanzu Mission Control. Si lo hace, podrá aprovisionar y administrar los clústeres de Tanzu Kubernetes mediante Tanzu Mission Control.

Para obtener más información sobre Tanzu Mission Control, consulte Administrar el ciclo de vida de los clústeres de Tanzu Kubernetes. Para ver una demostración, vea el vídeo Tanzu Mission Control integrado con el servicio Tanzu Kubernetes Grid.

Ver el espacio de nombres de Tanzu Mission Control en el clúster supervisor

vSphere with Tanzu v7.0.1 U1 y las versiones posteriores se distribuyen con un espacio de nombres de vSphere para Tanzu Mission Control. Este espacio de nombres se encuentra en el clúster supervisor donde se instala el agente de Tanzu Mission Control. Una vez se instala el agente, podrá aprovisionar y administrar los clústeres de Tanzu Kubernetes mediante la interfaz web de Tanzu Mission Control.

1 Utilice complemento de vSphere para kubectl para autenticarse en clúster supervisor. Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

2 Cambie el contexto al clúster supervisor, por ejemplo:

```
kubectl config use-context 10.199.95.59
```

3 Ejecute el siguiente comando para enumerar los espacios de nombres.

```
kubectl get ns
```

4 El espacio de nombres de vSphere que se proporciona para Tanzu Mission Control se identifica como `svc-tmc-cXX` (donde XX es un número).

5 Instale el agente de Tanzu Mission Control en este espacio de nombres. Consulte Instalar el agente de Tanzu Mission Control en el clúster supervisor.

Instalar el agente de Tanzu Mission Control en el clúster supervisor

Para integrar servicio Tanzu Kubernetes Grid con Tanzu Mission Control, instale el agente en el clúster supervisor.

Nota El siguiente procedimiento requiere vSphere 7.0 U3 con la versión 1.21.0 o posterior de clúster supervisor.

1 Mediante la interfaz web de Tanzu Mission Control, registre el clúster supervisor con Tanzu Mission Control. Consulte Registrar un clúster de administración en Tanzu Mission Control.

2 Mediante la interfaz web de Tanzu Mission Control, obtenga la URL de registro. Para ello, vaya a **Administración > Clústeres de administración**.

3 Abra un puerto de firewall en el entorno de vSphere with Tanzu para el puerto que requiere Tanzu Mission Control (normalmente `443`). Consulte Conexiones salientes realizadas por las extensiones del agente de clúster.

4 Inicie sesión en su entorno de vSphere with Tanzu mediante vSphere Client.

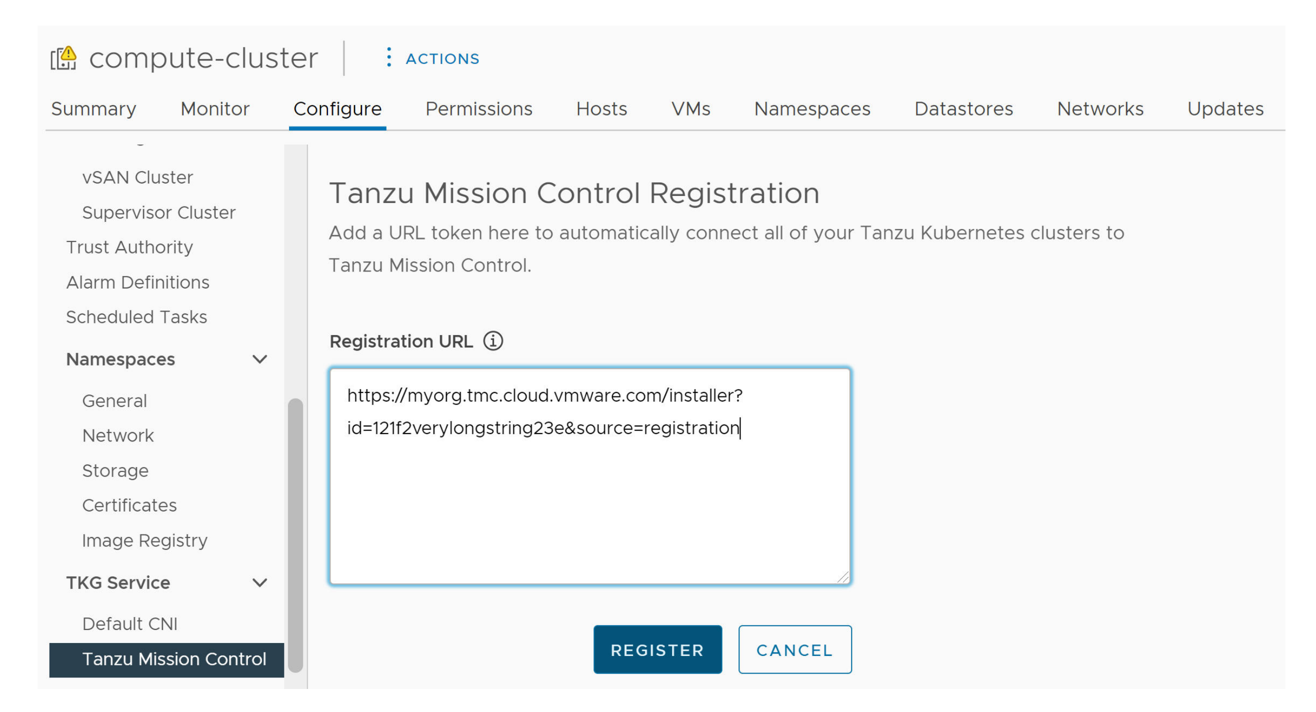
5 Seleccione el clúster de vCenter en el que está habilitada **Administración de cargas de trabajo**.

6 Seleccione la pestaña **Configurar**.

7 Seleccione **Servicio de TKG > Tanzu Mission Control**.

8 Proporcione la URL de registro en el campo **URL de registro**.

9 Haga clic en **Registrar**.



Desinstale el agente de Tanzu Mission Control

Si quiere desinstalar el agente de Tanzu Mission Control del clúster supervisor, consulte Eliminar manualmente el agente de clúster de un clúster supervisor en vSphere with Tanzu.

Configurar la CNI predeterminada para los clústeres de Tanzu Kubernetes

Como administrador vSphere, puede establecer la interfaz de red de contenedor (Container Network Interface, CNI) predeterminada para los clústeres de Tanzu Kubernetes.

CNI predeterminada

servicio Tanzu Kubernetes Grid admite dos opciones de CNI para clústeres de Tanzu Kubernetes: Antrea y Calico.

La CNI predeterminada definida por el sistema es Antrea. Para obtener más información sobre la configuración de la CNI predeterminada, consulte Parámetros de configuración para la API v1alpha1 de servicio Tanzu Kubernetes Grid.

Puede cambiar la CNI predeterminada mediante el vSphere Client. Para establecer la CNI predeterminada, complete el siguiente procedimiento.

Precaución Cambiar la CNI predeterminada es una operación global. El valor predeterminado recién establecido se aplica a todos los clústeres nuevos creados por el servicio. Los clústeres existentes no se modifican.

---

1 Inicie sesión en su entorno de vSphere with Tanzu mediante vSphere Client.

2 Seleccione el clúster de vCenter en el que está habilitada la administración de cargas de trabajo.

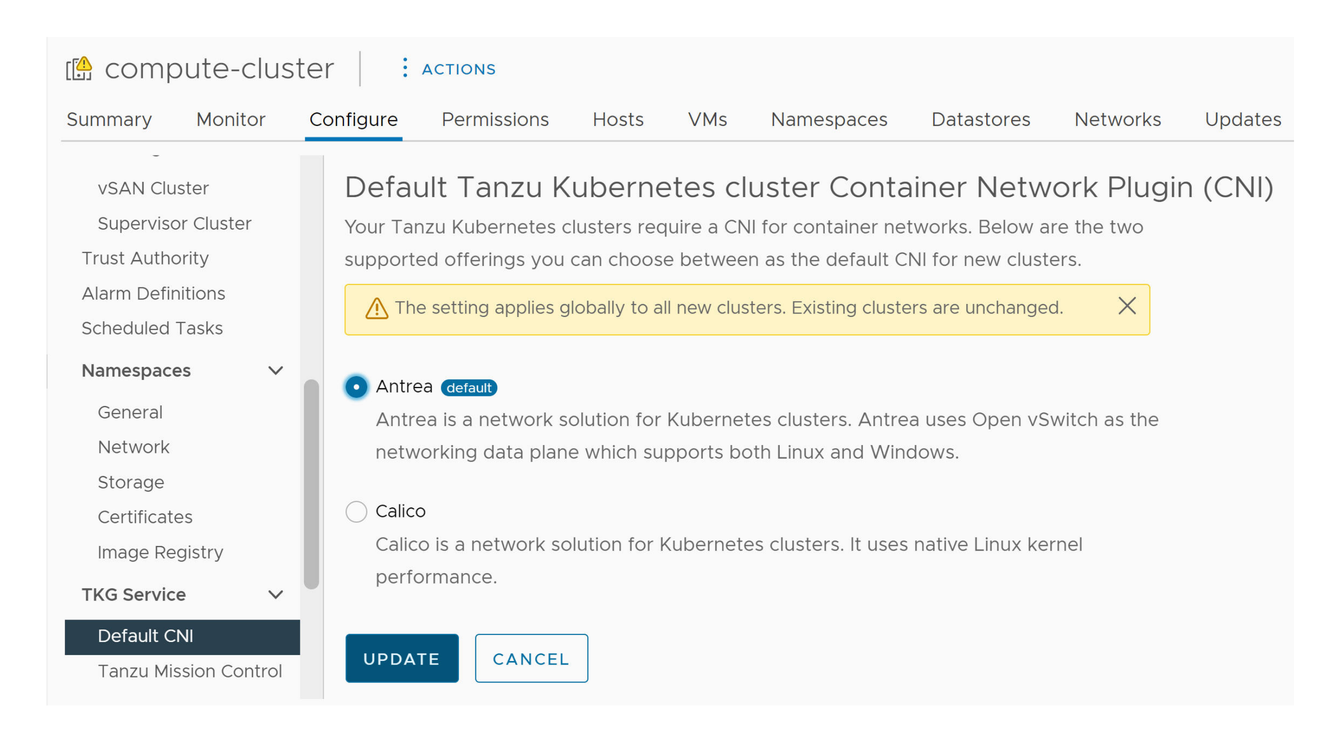
3 Seleccione la pestaña **Configurar**.

4 Seleccione **TKG Service > CNI predeterminada**.

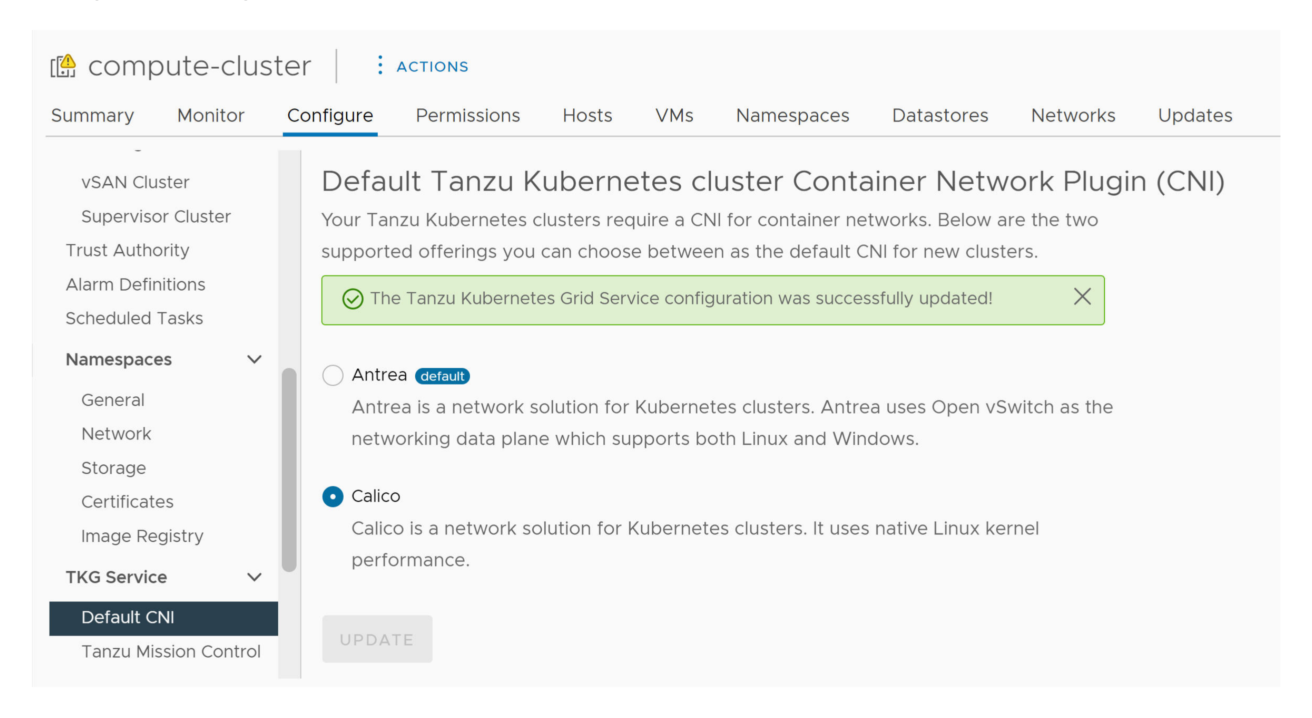
5 Elija la CNI predeterminada para los nuevos clústeres.

6 Haga clic en **Actualizar**.

La siguiente imagen muestra la selección de CNI predeterminada.



La siguiente imagen muestra cómo cambiar la selección de CNI de Antrea a Calico.



Agregar redes de cargas de trabajo a un clúster supervisor configurada con redes de VDS

Para un clúster supervisor configurada con la pila de redes vSphere, puede proporcionar aislamiento de Capa 2 para las cargas de trabajo de Kubernetes mediante la creación de redes de cargas de trabajo y su asignación a espacios de nombres. Las redes de cargas de trabajo proporcionan conectividad a los clústeres de Tanzu Kubernetes en el espacio de nombres y están

respaldadas por grupos de puertos distribuidos en el conmutador que está conectado a los hosts de clúster supervisor.

Para obtener más información sobre las topologías que puede implementar para clúster supervisor, consulte Topología para clúster supervisor con redes de vSphere y NSX Advanced Load Balancer o Topologías para implementar el equilibrador de carga de HAProxy.

Nota Si configuró clúster supervisor con un servidor DHCP que proporciona la configuración de redes para redes de cargas de trabajo, no podrá crear nuevas redes de cargas de trabajo después de la configuración de clúster supervisor.

Requisitos previos

- Cree un grupo de puertos distribuidos que respaldará la red de cargas de trabajo.
- Compruebe que el rango de IP que va a asignar a la red de cargas de trabajo sea único dentro de todas las instancias de clúster supervisor disponibles en su entorno.

Procedimiento

1 En vSphere Client, desplácese hasta clúster supervisor.

2 Seleccione **Configurar**.

3 En **Clúster supervisor**, seleccione **Red**.

4 Seleccione **Red de carga de trabajo** y haga clic en **Agregar**.

Opción	Descripción
Grupo de puertos	Seleccione el grupo de puertos distribuidos que se asociará con esta red de cargas de trabajo. El conmutador vSphere Distributed Switch (VDS) que está configurada para la red de **Clúster supervisor** contiene los grupos de puertos entre los que puede seleccionar.
Nombre de red	El nombre de red que identifica la red de cargas de trabajo cuando se asigna a espacios de nombres. Este valor se rellena automáticamente a partir del nombre del grupo de puertos que seleccione, pero puede cambiarlo según corresponda.
Rangos de direcciones IP	Introduzca un rango de IP para asignar direcciones IP de nodos del clúster Tanzu Kubernetes. El rango de IP debe estar en la subred indicada por la máscara de subred. **Nota** Debe utilizar rangos de direcciones IP únicos para cada red de cargas de trabajo. No configure los mismos rangos de direcciones IP para varias redes.

Opción	Descripción
Máscara de subred	Introduzca la dirección IP de la máscara de subred de la red en el grupo de puertos.
Puerta de enlace	Introduzca la puerta de enlace predeterminada para la red en el grupo de puertos. La puerta de enlace debe estar en la subred indicada por la máscara de subred. **Nota** No utilice la puerta de enlace que está asignada al equilibrador de carga de HAProxy.

5 Haga clic en **Agregar**.

Pasos siguientes

Asigne la red de cargas de trabajo recién creada a las instancias de espacio de nombres de vSphere.

Cambiar el tamaño del plano de control de un clúster supervisor

Compruebe cómo cambiar el tamaño de las máquinas virtuales del plano de control de Kubernetes de un clúster supervisor en el entorno de vSphere with Tanzu.

Requisitos previos

- Compruebe que tenga el privilegio **Modificar configuración de todo el clúster** en el clúster.

Procedimiento

1 En vSphere Client, desplácese hasta clúster supervisor.

2 Seleccione **Configurar** y haga clic en **General**.

3 Expanda **Tamaño del plano de control**, haga clic en **Editar** y seleccione nuevo tamaño de plano de control en el menú desplegable.

4 Haga clic en **Guardar**.

   Solo puede escalar verticalmente el tamaño del plano de control.

Cambiar la configuración de red de administración en un clúster supervisor

Aprenda a actualizar la configuración de DNS y NTP en la red de administración de clúster supervisor en el entorno de vSphere with Tanzu.

Requisitos previos

- Compruebe que tenga el privilegio **Modificar configuración de todo el clúster** en el clúster.

Procedimiento

1 En vSphere Client, desplácese hasta clúster supervisor.

2 Seleccione **Configurar**.

3 En **Clúster supervisor**, seleccione **Red**.

4 Haga clic en **Red de administración**.

5 Edite la configuración de DNS y NTP.

Opción	Descripción
Servidor(es) DNS	Introduzca las direcciones de los servidores DNS que utiliza en su entorno. Si el sistema vCenter Server está registrado con un FQDN, debe introducir las direcciones IP de los servidores DNS que utiliza con el entorno de vSphere para que el FQDN se pueda resolver en el clúster supervisor.
Dominio(s) de búsqueda de DNS	Introduzca los nombres de dominio que DNS busca dentro de los nodos del plano de control de Kubernetes, como `corp.local`, para que el servidor DNS pueda resolverlos.
Servidor(es) NTP	Introduzca las direcciones de los servidores NTP que utiliza en su entorno, si los hubiera.

Cambiar la configuración de red de carga de trabajo en un clúster supervisor configurada con redes de VDS

Consulte cómo cambiar la configuración del servidor NTP y DNS para las redes de cargas de trabajo de un clúster supervisor configurada con la pila de redes de VDS. Los servidores DNS que se configuran para las redes de cargas de trabajo son servidores DNS externos expuestos a cargas de trabajo de Kubernetes y resuelven los nombres de dominio predeterminados que se alojan fuera del clúster supervisor.

Requisitos previos

- Compruebe que tenga el privilegio **Modificar configuración de todo el clúster** en el clúster.

Procedimiento

1 En vSphere Client, desplácese hasta clúster supervisor.

2 Seleccione **Configurar**.

3 En **Clúster supervisor**, seleccione **Red**.

4 Seleccione **Red de carga de trabajo**.

5 Edite la configuración del servidor DNS.

   Introduzca las direcciones de los servidores DNS que pueden resolver los nombres de dominio de los componentes de administración de vSphere, como por ejemplo vCenter Server.

   Por ejemplo, **`10.142.7.1`**.

Al introducir la dirección IP del servidor DNS, se agrega una ruta estática a cada máquina virtual del plano de control. Esto indica que el tráfico a los servidores DNS pasa por la red de cargas de trabajo.

Si los servidores DNS que especifica se comparten entre la red de administración y la red de cargas de trabajo, las búsquedas de DNS en las máquinas virtuales del plano de control se enrutan a través de la red de cargas de trabajo después de la configuración inicial.

6 Edite la configuración de NTP según sea necesario.

Cambiar la configuración de red de carga de trabajo en un clúster supervisor configurada con NSX-T Data Center

Aprenda a cambiar la configuración de redes para el servidor DNS, las redes de espacio de nombres, la entrada y la salida de un clúster supervisor configurada para NSX-T Data Center como la pila de redes.

Requisitos previos

- Compruebe que tenga el privilegio **Modificar configuración de todo el clúster** en el clúster.

Procedimiento

1 En vSphere Client, desplácese hasta clúster supervisor.

2 Seleccione **Configurar**.

3 En **Clúster supervisor**, seleccione **Red**.

4 Seleccione **Red de carga de trabajo**.

5 Cambie la configuración de redes según sea necesario.

Opción	Descripción
Servidor(es) DNS	Introduzca las direcciones de los servidores DNS que pueden resolver los nombres de dominio de los componentes de administración de vSphere, como por ejemplo vCenter Server. Por ejemplo, `10.142.7.1`. Cuando se introduce la dirección IP del servidor DNS, se agrega una ruta estática a cada máquina virtual del plano de control. Esto indica que el tráfico a los servidores DNS pasa por la red de cargas de trabajo. Si los servidores DNS que especifica se comparten entre la red de administración y la red de cargas de trabajo, las búsquedas de DNS en las máquinas virtuales del plano de control se enrutan a través de la red de cargas de trabajo después de la configuración inicial.
Red de espacio de nombres	Introduzca una anotación CIDR para cambiar el rango de IP de las cargas de trabajo de Kubernetes que están asociadas a los segmentos de espacio de nombres del clúster supervisor. Si el modo NAT no está configurado, este rango de CIDR de IP debe ser una dirección IP enrutable.

Opción	Descripción
Ingreso	Introduzca una anotación CIDR para cambiar el rango de IP de entrada de los servicios de Kubernetes. Este rango se utiliza para los servicios de tipo equilibrador de carga y entrada. Para los clústeres deTanzu Kubernetes, la publicación de servicios a través del equilibrador de carga ServiceType también obtendrá las direcciones IP de este bloque CIDR de IP. **Nota** Solo puede agregar los CIDR a los campos de red de entrada y carga de trabajo, pero no puede editar ni eliminar los existentes.
Egreso	Introduzca una anotación CIDR para asignar direcciones IP para la Traducción de Direcciones de Red de Origen (Source Network Address Translation, SNAT) para el tráfico que sale del clúster supervisor para acceder a servicios externos. Solo se asigna una dirección IP de egreso para cada espacio de nombres en el clúster supervisor. La IP de salida es la dirección IP que los pods de vSphere en el espacio de nombres concreto usan para comunicarse fuera del NSX-T Data Center.

Resolución de estados de errores en clúster supervisor durante la configuración inicial o la actualización

Después de configurar inicialmente un clúster de vSphere como clúster supervisor o de actualizar o editar la configuración de un clúster supervisor existente, toda la configuración que haya especificado se validará y se aplicará al clúster hasta que se complete la configuración. Las comprobaciones de estado se realizan en los parámetros introducidos que pueden detectar errores en la configuración, lo que da como resultado un estado de error de clúster supervisor. Debe resolver estos estados de error para que se pueda reanudar la configuración o la actualización del clúster supervisor.

Puede ver el estado del clúster supervisor en vSphere Client, en **Administración de cargas de trabajo > Clústeres supervisores** El estado de la configuración del clúster se muestra en la columna **Estado de configuración**.

Tabla 5-1. Errores de conexión de vCenter Server

Mensaje de error	Motivo	Solución
No se puede resolver el identificador de red principal de vCenter <*FQDN*> con los servidores DNS de administración configurados en la máquina virtual del plano de control <*nombre de la máquina virtual*>. Valide que los servidores DNS de administración <nombre del servidor> puedan resolver <*nombre de la red*>.	■ Se puede acceder al menos a un servidor DNS de administración. ■ Se proporciona al menos un DNS de administración de forma estática. ■ Los servidores DNS de administración no tienen ninguna búsqueda de nombre de host para el PNID de vCenter Server. ■ El PNID de vCenter Server es un nombre de dominio, no una dirección IP estática.	■ Agregue una entrada de host para el PNID de vCenter Server a los servidores DNS de administración. ■ Compruebe que los servidores DNS configurados sean correctos.
No se puede resolver el identificador de red principal de vCenter <*nombre de la red*> con los servidores DNS adquiridos a través de DHCP en la red de administración de la máquina virtual del plano de control <*nombre de la máquina virtual*>. Valide que los servidores DNS de administración puedan resolver <*nombre de la red*>.	■ Se puede acceder a los servidores DNS de administración suministrados por el servidor DHCP (al menos uno). ■ Los servidores DNS de administración se suministran de forma estática. ■ Los servidores DNS de administración no tienen ninguna búsqueda de nombre de host para el PNID de vCenter Server. ■ Los servidores DNS de administración no tienen ninguna búsqueda de nombre de host para el PNID de vCenter Server. ■ El PNID de vCenter Server es un nombre de dominio, no una dirección IP estática.	■ Agregue una entrada de host para el PNID de vCenter Server a los servidores DNS de administración suministrados por el servidor DHCP configurado. ■ Compruebe que los servidores DNS que proporciona el servidor DHCP sean correctos.
No se puede resolver el host<*nombre del host*> en la máquina virtual del plano de control <*nombre de la máquina virtual*, ya que no hay servidores DNS de administración configurados.	■ El PNID de vCenter Server es un nombre de dominio, no una dirección IP estática. ■ No hay servidores DNS configurados.	Configure un servidor DNS de administración.
No se puede resolver el host <*nombre del host*> en la máquina virtual del plano de control <*nombre de la máquina virtual*>. El nombre de host termina con el dominio de nivel superior '.local', que requiere que se incluya 'local' en los dominios de búsqueda de DNS de administración.	El PNID de vCenter Server contiene `.local` como dominio de nivel superior (top-level domain, TLD), pero los dominios de búsqueda configurados no incluyen `local.`	Agregue `local` a los dominios de búsqueda de DNS de administración.

Tabla 5-1. Errores de conexión de vCenter Server (continuación)

Mensaje de error	Motivo	Solución
No se puede conectar a los servidores DNS de administración <*nombre del servidor*> desde la máquina virtual del plano de control <*nombre de la máquina virtual*>. Se intentó la conexión a través de la red de carga de trabajo.	■ Los servidores DNS de administración no se pueden conectar a vCenter Server. ■ Los valores de `worker_dns` proporcionados contienen en su totalidad los valores de DNS de administración proporcionados. Esto significa que el tráfico se enruta a través de la red de carga de trabajo, ya que clúster supervisor debe elegir una interfaz de red para dirigir el tráfico estático a estas direcciones IP.	■ Compruebe la red de carga de trabajo para verificar que se puede enrutar a los servidores DNS de administración configurados. ■ Compruebe que no haya direcciones IP en conflicto que puedan activar el enrutamiento alternativo entre los servidores DNS y otros servidores de la red de carga de trabajo. ■ Compruebe que el servidor DNS configurado sea, de hecho, un servidor DNS y que aloje su puerto DNS en el puerto 53. ■ Compruebe que los servidores DNS de carga de trabajo estén configurados para permitir conexiones desde las direcciones IP de las máquinas virtuales del plano de control (las direcciones IP proporcionadas por la red de carga de trabajo). ■ Compruebe que no haya errores ortográficos en las direcciones de los servidores DNS de administración. ■ Compruebe que los dominios de búsqueda no incluyan un '~' innecesario que podría estar resolviendo el nombre de host de forma incorrecta.

Tabla 5-1. Errores de conexión de vCenter Server (continuación)

Mensaje de error	Motivo	Solución
No se puede conectar a los servidores DNS de administración <*nombre del servidor*> desde la máquina virtual del plano de control <*nombre de la máquina virtual*>.	No se puede conectar a los servidores DNS.	■ Revise la red de administración para comprobar que existen rutas a los servidores DNS de administración. ■ Compruebe que no haya direcciones IP en conflicto que puedan activar el enrutamiento alternativo entre los servidores DNS y otros servidores. ■ Compruebe que el servidor DNS configurado sea, de hecho, un servidor DNS y que aloje su puerto DNS en el puerto 53. ■ Compruebe que los servidores DNS de administración estén configurados para permitir conexiones desde las direcciones IP de las máquinas virtuales del plano de control. ■ Compruebe que no haya errores ortográficos en las direcciones de los servidores DNS de administración. ■ Compruebe que los dominios de búsqueda no incluyan un '~' innecesario que podría estar resolviendo el nombre de host de forma incorrecta.
No se puede conectar a <*nombre del componente*> <*dirección del componente*> desde la máquina virtual del plano de control <nombre de la máquina virtual>. Error: *texto del mensaje de error*	■ Se produjo un error de red genérico. ■ Se produjo un error al conectarse a la conexión real a vCenter Server.	■ Valide que el nombre de host o la dirección IP de los componentes configurados, como vCenter Server, HAProxy, NSX Manager o NSX Advanced Load Balancer, sean correctos. ■ Valide cualquier configuración de red externa, como direcciones IP en conflicto, reglas de firewall y otras, en la red de administración.

Tabla 5-1. Errores de conexión de vCenter Server (continuación)

Mensaje de error	Motivo	Solución
La máquina virtual del plano de control <*nombre de la máquina virtual*> no pudo validar el certificado de vCenter <*nombre de vCenter Server*>. El certificado de vCenter Server no es válido.	El certificado proporcionado por vCenter Server tiene un formato no válido y, por lo tanto, no es de confianza.	■ Reinicie `wcpsvc` para comprobar que el paquete de raíces de confianza en las máquinas virtuales del plano de control esté actualizado con los certificados raíz de vCenter Server más recientes. ■ Compruebe que el certificado de vCenter Server sea válido.
La máquina virtual del plano de control <*nombre de la máquina virtual*> no confía en el certificado de vCenter <*nombre de vCenter Server*>.	■ El certificado `vmca.pem` que presenta vCenter Server es diferente de lo que está configurado para las máquinas virtuales del plano de control. ■ Los certificados raíz de confianza se reemplazaron en el dispositivo de vCenter Server, pero `wcpsvc` no se reinició.	■ Reinicie `wcpsvc` para comprobar que el paquete de raíces de confianza en las máquinas virtuales del plano de control esté actualizado con las raíces de certificado de vCenter Server más recientes.

Tabla 5-2. Errores de conexión de NSX Manager

La máquina virtual del plano de control <*nombre de la máquina virtual*> no pudo validar el certificado del servidor NSX <*nombre del servidor NSX*>. La huella digital que devuelve el servidor <*dirección de NSX-T*> no coincide con la huella digital de certificado del cliente esperada registrada en vCenter <*nombre de vCenter Server*>	Las huellas digitales SSL registradas en el clúster supervisor no coinciden con el hash SHA-1 del certificado que presenta NSX Manager.	■ Vuelva a habilitar la confianza en NSX Manager entre NSX y la instancia de vCenter Server. ■ Reinicie `wcpsvc` en vCenter Server.
No se puede conectar a <*nombre del componente*> <*dirección del componente*> desde la máquina virtual del plano de control <*nombre de la máquina virtual*>. Error: *texto del mensaje de error*	Se produjo un error de red genérico.	■ Valide cualquier configuración de red externa, direcciones IP en conflicto, reglas de firewall y otros elementos en la red de administración para NSX Manager. ■ Compruebe que la dirección IP de NSX Manager en la extensión de NSX sea correcta. ■ Compruebe que NSX Manager se esté ejecutando.

Tabla 5-3. Errores del equilibrador de carga

La máquina virtual del plano de control <*nombre de máquina virtual*> no confía en el certificado del equilibrador de carga (<*equilibrador de carga*> - <*endpoint del equilibrador de carga*>).	El certificado que presenta el equilibrador de carga es diferente del certificado que está configurado para las máquinas virtuales del plano de control.	Compruebe que haya configurado el certificado TLS de administración correcto para el equilibrador de carga.
La máquina virtual del plano de control <*nombre de máquina virtual*> no pudo validar el certificado del equilibrador de carga (<*equilibrador de carga*> - <*endpoint del equilibrador de carga*>. El certificado no es válido.	El certificado que presenta el equilibrador de carga tiene un formato no válido o ha caducado.	Corrija el certificado del servidor del equilibrador de carga configurado.
La máquina virtual del plano de control <*nombre de la máquina virtual*> no pudo autenticarse en el equilibrador de carga (<*equilibrador de carga*> - <*endpoint del equilibrador de carga*> con el nombre de usuario <*nombre de usuario*> y la contraseña proporcionada.	El nombre de usuario o la contraseña del equilibrador de carga son incorrectos.	Compruebe si el nombre de usuario y la contraseña configurados en el equilibrador de carga son correctos.
Se produjo un error de HTTP al intentar conectarse al equilibrador de carga (<*equilibrador de carga*> - <*endpoint del equilibrador del carga*> desde la máquina virtual del plano de control <*nombre de la máquina virtual*>).	Las máquinas virtuales del plano de control pueden conectarse al endpoint del equilibrador de carga, pero el endpoint no devuelve una respuesta http correcta (200).	Compruebe que el equilibrador de carga esté en buen estado y acepte solicitudes.
No se puede conectar al <*equilibrador de carga*> (<*endpoint del equilibrador de carga*>) desde la máquina virtual del plano de control <*nombre de la máquina virtual*>. Error: <*texto de error*>	■ Se produjo un error de red genérico. ■ Por lo general, significa que el equilibrador de carga no funciona o que algún firewall bloquea la conexión.	■ Validar que se puede acceder al endpoint del equilibrador de carga ■ Valide que no haya firewalls que bloqueen la conexión con el equilibrador de carga.

Configuración de los ajustes del proxy HTTP en vSphere with Tanzu

Descubra cómo configurar los ajustes del proxy HTTP para los clústeres de clústeres supervisor y Tanzu Kubernetes. Conozca cuál es el flujo de trabajo para configurar el proxy HTTP para clústeres de clústeres supervisor y Tanzu Kubernetes cuando los registre en Tanzu Mission Control. Utilice un proxy HTTP para extraer imágenes y tráfico de contenedor para clústeres supervisor locales que registre como clústeres de administración en Tanzu Mission Control.

Flujo de trabajo para configurar los ajustes del proxy HTTP en clústeres de clústeres supervisor y Tanzu Kubernetes para usarlos con Tanzu Mission Control

Para configurar un proxy HTTP en clústeres supervisor que desea registrar como clústeres de administración con Tanzu Mission Control, siga los pasos que se indican a continuación:

1 En vSphere, configure el proxy HTTP en clústeres supervisor heredando la configuración del proxy HTTP de vCenter Server o configurando los ajustes del proxy en clústeres supervisor individuales a través de la línea de comandos DCLI o las API de clústeres de administración de espacios de nombres.

2 En Tanzu Mission Control, cree un objeto de configuración de proxy mediante los ajustes de proxy que configuró para los clústeres supervisor en vSphere with Tanzu. Consulte Crear un objeto de configuración de proxy para un clúster del servicio Tanzu Kubernetes Grid que se ejecuta en vSphere with Tanzu.

3 En Tanzu Mission Control, utilice este objeto de configuración de proxy cuando registre clústeres supervisor como clúster de administración. Consulte Registrar un clúster de administración con Tanzu Mission Control y Completar el registro de un clúster supervisor en vSphere with Tanzu.

Para configurar un proxy HTTP para clústeres de Tanzu Kubernetes que aprovisione o agregue como clústeres de carga de trabajo en Tanzu Mission Control:

1 Cree un objeto de configuración de proxy con la configuración de proxy que desea utilizar con clústeres de Tanzu Kubernetes. Consulte Crear un objeto de configuración de proxy para un clúster del servicio Tanzu Kubernetes Grid que se ejecuta en vSphere with Tanzu.

2 Utilice ese objeto de configuración de proxy cuando aprovisione o agregue clústeres de Tanzu Kubernetes como clústeres de carga de trabajo. Consulte Aprovisionar un clúster en vSphere with Tanzu y Agregar un clúster de carga de trabajo a Tanzu Mission Control Management

Configurar un proxy HTTP para clústeres de Tanzu Kubernetes en vSphere with Tanzu

Utilice uno de los siguientes métodos para configurar un proxy para los clústeres de Tanzu Kubernetes en vSphere with Tanzu:

- Configure los ajustes de proxy para clústeres de Tanzu Kubernetes individuales. Consulte Parámetros de configuración para aprovisionar clústeres de Tanzu Kubernetes mediante la API del servicio Tanzu Kubernetes Grid v1alpha2. Para ver un ejemplo de YAML de configuración, consulte Ejemplo de YAML para aprovisionar un clúster personalizado de Tanzu Kubernetes mediante la API del servicio Tanzu Kubernetes Grid v1alpha2.

- Cree una configuración de proxy global que se aplicará a todos los clústeres de Tanzu Kubernetes. Consulte Parámetros de configuración para la API del servicio Tanzu Kubernetes Grid v1alpha2.

Nota Si utiliza Tanzu Mission Control para administrar los clústeres de Tanzu Kubernetes, no es necesario configurar los ajustes de proxy a través del archivo YAML del clúster en vSphere with Tanzu. Puede configurar los ajustes de proxy cuando agregue los clústeres de Tanzu Kubernetes como clústeres de carga de trabajo a Tanzu Mission Control.

Configurar los ajustes del proxy en clústeres supervisor de vSphere 7.0 Update 3 creados recientemente

Para los clústeres supervisor creados recientemente en un entorno de vSphere 7.0 Update 3, la configuración del proxy HTTP se hereda de vCenter Server. Independientemente de si crea clústeres supervisor antes o después de configurar los ajustes del proxy HTTP en vCenter Server, los clústeres heredan la configuración.

Consulte Configurar los ajustes de DNS, dirección IP y proxy para obtener información sobre cómo configurar los ajustes del proxy HTTP en vCenter Server.

También puede anular la configuración del proxy HTTP heredado en clústeres supervisor individuales a través de la API de administración de clústeres o DCLI.

Dado que heredar la configuración del proxy de vCenter Server es la configuración predeterminada para los clústeres supervisor de vSphere 7.0.3 creados recientemente, también puede utilizar la API de administración del clúster o DCLI para no heredar ninguna configuración de proxy HTTP en caso de que los clústeres supervisor no requieran un proxy, pero vCenter Server sigue requiriéndolo.

Configurar los ajustes del proxy en clústeres supervisor actualizados a vSphere 7.0 Update 3

Si actualizó clústeres supervisor a vSphere 7.0 Update 3, la configuración del proxy HTTP de vCenter Server no se hereda automáticamente. En ese caso los ajustes de proxy de clústeres supervisor se configuran mediante la línea de comandos DCLI o la API `vcenter/namespace-management/clusters`.

Usar la API de administración de clústeres para configurar el proxy HTTP en clústeres supervisor

Los ajustes de proxy de clúster supervisor se configuran a través de la API de `vcenter/namespace-management/clusters`. La API proporciona tres opciones para la configuración de proxy en clúster supervisor:

Configuración de API	clústeres supervisor de vSphere 7.0.3 creados recientemente	clústeres supervisor actualizados a vSphere 7.0.3
`VC_INHERITED`	Este es el ajuste predeterminado para los nuevos clústeres supervisor y no es necesario utilizar la API para configurar los ajustes de proxy de los clústeres supervisor. Solo puede configurar los ajustes de proxy de los vCenter Server a través de su interfaz de administración.	Utilice esta opción para insertar la configuración del proxy HTTP en los clústeres supervisor actualizados a vSphere 7.0.3.
`CLUSTER_CONFIGURED`	Utilice esta opción para anular la configuración de proxy HTTP heredada de vCenter Server en uno de los siguientes casos: ■ Se requiere un clúster supervisor en una subred diferente a vCenter Server y se requiere un servidor proxy diferente. ■ El servidor proxy utiliza paquetes de CA personalizados.	Utilice esta opción para configurar el proxy HTTP para clústeres supervisor individuales actualizados a vSphere 7.0.3 en uno de los siguientes casos: ■ No se puede utilizar el proxy de vCenter Server porque clúster supervisor reside en una subred diferente a vCenter Server y se requiere un servidor proxy diferente. ■ El servidor proxy utiliza paquetes de CA personalizados.
`NONE`	Utilice esta opción cuando clúster supervisor tenga conectividad directa a Internet mientras vCenter Server requiera un proxy. El ajuste NINGUNO impide que vCenter Server herede la configuración de proxy de los clústeres supervisor.	

Para establecer un proxy HTTP para un clúster supervisor o modificar la configuración existente, utilice los siguientes comandos en una sesión SSH con vCenter Server :

```
vc_address=<IP address>
cluster_id=domain-c<number>
session_id=$(curl -ksX POST --user '<SSO user name>:<password>' https://$vc_address/api/
session | xargs -t)
curl -k -X PATCH -H "vmware-api-session-id: $session_id" -H "Content-Type: application/
json" -d '{ "cluster_proxy_config": { "proxy_settings_source": "CLUSTER_CONFIGURED",
"http_proxy_config":"<proxy_url>" } }' https://$vc_address/api/vcenter/namespace-management/
clusters/$cluster_id
```

Solo es necesario transferir el `domain_c<number>` del identificador de clúster completo. Por ejemplo, tome `domain-c50` del siguiente identificador de clúster: `ClusterComputeResource:domain-c50:5bbb510f-759f-4e43-96bd-97fd703b4edb`.

Cuando utilice la configuración de `VC_INHERITED` o `NONE`, omita `"http_proxy_config:<proxy_url>"` en el comando.

Para utilizar un paquete de CA personalizado, agregue `"tlsRootCaBundle": "<TLS_certificate>"` al comando proporcionando el certificado de CA de TSL en texto sin formato.

Usar DCLI para configurar los ajustes del proxy HTTP en clústeres supervisor

Puede usar el siguiente comando DCLI para configurar los ajustes del proxy HTTP para clústeres supervisor mediante la opción `CLUSTER_CONFIGURED`.

```
<dcli> namespacemanagement clusters update --cluster domain-c57 --cluster-proxy-config-http-proxy-config <proxy URL> --cluster-proxy-config-https-proxy-config <proxy URL> --cluster-proxy-config-proxy-settings-source CLUSTER_CONFIGURED
```

Transmitir registros del plano de control de clúster supervisor a un rsyslog remoto

Compruebe cómo configurar la transmisión de registros desde las máquinas virtuales del plano de control de clúster supervisor hacia un receptor rsyslog remoto para evitar la pérdida de datos de registro valiosos.

Los registros generados por los componentes en las máquinas virtuales del plano de control de clúster supervisor se almacenan localmente en los sistemas de archivos de las máquinas virtuales. Cuando se acumula una gran cantidad de registros, los registros se rotan a alta velocidad, lo que provoca la pérdida de mensajes valiosos que pueden ayudar a identificar la causa principal de diferentes problemas. vCenter Server y las máquinas virtuales del plano de control de clúster supervisor admiten la transmisión de sus registros locales a un receptor rsyslog remoto. Esta función ayuda a capturar registros para los siguientes servicios y componentes:

- En vCenter Server: servicio del plano de control de carga de trabajo, servicio de ESX Agent Manager, servicio de entidad de certificación y todos los demás servicios que se ejecutan en vCenter Server.
- Componentes del plano de control de clúster supervisor y servicios integrados de clúster supervisor, como el servicio de máquina virtual, y servicio Tanzu Kubernetes Grid.

Puede configurar el dispositivo de vCenter Server para recopilar y transmitir datos de registro locales a un receptor rsyslog remoto. Una vez que esta configuración se aplica a vCenter Server, el remitente de rsyslog que se ejecuta dentro de vCenter Server comienza a enviar registros generados por los servicios dentro de ese sistema vCenter Server.

clúster supervisor utiliza el mismo mecanismo que vCenter Server para descargar registros locales con el fin de reducir la sobrecarga de administración de la configuración. El servicio del plano de control de carga de trabajo supervisa la configuración de rsyslog de vCenter Server mediante registros de sondeo periódicamente. Si el servicio del plano de control de carga de trabajo detecta que la configuración de rsyslog del vCenter Server remoto no está vacía, el servicio propaga esta configuración a cada máquina virtual del plano de control en todos los clústeres supervisor. Esto puede generar una gran cantidad de tráfico de mensajes rsyslog que puede sobrecargar al receptor rsyslog remoto. Por lo tanto, la máquina receptora debe tener suficiente capacidad de almacenamiento para soportar grandes cantidades de mensajes rsyslog.

Al eliminar la configuración de rsyslog de vCenter Server, se detienen los mensajes rsyslog de vCenter Server. El servicio del plano de control de carga de trabajo detecta el cambio y lo propaga a cada máquina virtual del plano de control en cada clúster supervisor y detiene también los flujos de máquina virtual del plano de control.

Pasos de configuración

Realice los siguientes pasos para configurar la transmisión de rsyslog para máquinas virtuales del plano de control de clúster supervisor:

1. Configure un receptor rsyslog aprovisionando una máquina que:
   - Ejecuta el servicio rsyslog en modo receptor. Consulte el ejemplo Recuperar grandes cantidades de mensajes con alto rendimiento en la documentación de rsyslog.
   - Hay suficiente espacio de almacenamiento para alojar grandes cantidades de datos de registro.
   - Tiene conectividad de red para recibir datos de vCenter Server y las máquinas virtuales del plano de control de clúster supervisor.
2. Inicie sesión en la interfaz de administración del dispositivo de vCenter Server en *https://<dirección de vCenter Server>:5480* como raíz.
3. Configure vCenter Server para transmitir al receptor rsyslog a través de la interfaz de administración de dispositivos de vCenter Server. Consulte Reenviar archivos de registro de vCenter Server al servidor syslog remoto.

La configuración de rsyslog de vCenter Server puede tardar unos minutos en aplicarse a las máquinas virtuales del plano de control de clúster supervisor. El servicio del plano de control de carga de trabajo en el dispositivo de vCenter Server sondea la configuración del dispositivo cada 5 minutos y la propaga a todos los clústeres supervisor disponibles. La cantidad de tiempo necesaria para que se complete la propagación depende de la cantidad de clústeres supervisor en su entorno. En caso de que algunas de las máquinas virtuales del plano de control de los clústeres supervisor tengan un estado incorrecto o realicen otra operación, el servicio del plano de control de carga de trabajo volverá a intentar aplicar la configuración de rsyslog hasta que se realice correctamente.

Inspeccionar registros de los componentes de máquinas virtuales del plano de control

El rsyslog de las máquinas virtuales del plano de control de clúster supervisor inserta etiquetas en los mensajes de registro que indican el componente de origen de estos mensajes de registro.

Etiquetas de registro	Descripción
`vns-control-plane-pods <pod_name>/<instance_number>.log`	Registros que se originaron desde pods de Kubernetes en máquinas virtuales del plano de control. Por ejemplo: `vns-control-plane-pods etcd/0.log` o `vns-control-plane-pods nsx-ncp/573.log`
`vns-control-plane-imc`	Registros de configuración inicial de las máquinas virtuales del plano de control.
`vns-control-plane-boostrap`	Registros de arranque de la implementación del plano de control de los nodos de Kubernetes.
`vns-control-plane-upgrade-logs`	Registros de revisiones de nodos del plano de control y actualizaciones de versiones secundarias.
`vns-control-plane-svchost-logs`	Registros de agente o host del servicio de nivel de sistema de la máquina virtual del plano de control.
`vns-control-plane-update-controller`	Sincronizador de estado deseado del plano de control y registro de vRealize.
`vns-control-plane-compact-etcd-logs`	Registros para mantener la compactación del almacenamiento del servicio etcd del plano de control.

Crear y administrar bibliotecas de contenido en vSphere with Tanzu

6

Los objetos de vSphere with Tanzu, como máquinas virtuales independientes y clústeres de Tanzu Kubernetes, utilizan bibliotecas de contenido como repositorios centralizados para plantillas, imágenes, distribuciones y otros archivos relacionados con su implementación.

Este capítulo incluye los siguientes temas:

- Crear y administrar bibliotecas de contenido para versiones de Tanzu Kubernetes
- Crear y administrar bibliotecas de contenido para máquinas virtuales independientes en vSphere with Tanzu

Crear y administrar bibliotecas de contenido para versiones de Tanzu Kubernetes

VMware Tanzu distribuye las versiones de software de Kubernetes como versiones de Tanzu Kubernetes. Para consumir estas versiones, puede configurar una biblioteca de contenido de vSphere y sincronizar las versiones disponibles. Puede hacerlo mediante un modelo basado en suscripciones o a pedido. Si desea aprovisionar Tanzu Kubernetes en un entorno restringido de Internet, puede crear una biblioteca local e importar manualmente las versiones.

Acerca de las distribuciones de versión de Tanzu Kubernetes

Una versión de Tanzu Kubernetes proporciona la distribución de software de Kubernetes firmada y compatible con VMware para su uso con clústeres de Tanzu Kubernetes. Puede obtener y administrar versiones de Tanzu Kubernetes mediante una biblioteca de contenido de vSphere.

Cada versión de Tanzu Kubernetes se distribuye como una plantilla de OVA. El servicio Tanzu Kubernetes Grid utiliza la plantilla de OVA para construir los nodos de máquina virtual para clústeres de Tanzu Kubernetes.

Para obtener una lista de las versiones de Tanzu Kubernetes y la compatibilidad con el clúster supervisor, consulte las notas de la versión de Tanzu Kubernetes.

Se admite una versión de Tanzu Kubernetes en Photon OS y Ubuntu. El tamaño de disco de la máquina virtual creada a partir de la plantilla de OVA es fijo. Los recursos de CPU y RAM se especifican al aprovisionar un clúster de Tanzu Kubernetes. Consulte Clases de máquina virtual para clústeres de Tanzu Kubernetes.

El servicio Tanzu Kubernetes Grid extrae las plantillas de OVA de la versión de Tanzu Kubernetes de una biblioteca de contenido de vSphere. Puede utilizar una biblioteca de contenido suscrita para automatizar el proceso o una biblioteca de contenido local para entornos con acceso restringido a Internet. Consulte Crear, proteger y sincronizar una biblioteca de contenido suscrita para las versiones de Tanzu Kubernetes y Crear, proteger y sincronizar una biblioteca de contenido local para versiones de Tanzu Kubernetes.

El tamaño de la biblioteca de contenido puede aumentar con el tiempo, a medida que se publican nuevas versiones de Tanzu Kubernetes. Si el almacenamiento subyacente se queda sin espacio, puede migrar a una biblioteca de contenido nueva. Consulte Migrar clústeres de Tanzu Kubernetes a una nueva biblioteca de contenido.

Después de crear y sincronizar la biblioteca de contenido, configure cada espacio de nombres de vSphere en el que tiene pensado aprovisionar clústeres de Tanzu Kubernetes. Esto incluye asociar la biblioteca de contenido y las clases de máquinas virtuales con el espacio de nombres de vSphere. En este punto, puede iniciar sesión en el espacio de nombres de vSphere y comprobar que las versiones de Tanzu Kubernetes estén disponibles. Consulte Configurar un espacio de nombres de vSphere para las versiones de Tanzu Kubernetes.

Crear, proteger y sincronizar una biblioteca de contenido suscrita para las versiones de Tanzu Kubernetes

Para almacenar una versión de Tanzu Kubernetes para su uso con clústeres de Tanzu Kubernetes, cree una biblioteca de contenido suscrita en vCenter Server donde vSphere with Tanzu esté habilitado.

Una biblioteca de contenido suscrita se origina en una biblioteca de contenido publicada. Después de crear la suscripción, el sistema la sincronizará con la biblioteca publicada. Puede elegir el modo de sincronización: inmediato o a petición. Para obtener más información, consulte Administrar una biblioteca suscrita.

Requisitos previos

Revise Acerca de las distribuciones de versión de Tanzu Kubernetes.

Se requieren los siguientes privilegios de vSphere para crear una biblioteca de contenido:

- **Biblioteca de contenido.Crear biblioteca local** o **Biblioteca de contenido.Crear biblioteca suscrita** en la instancia de vCenter Server en la que desea crear la biblioteca.
- **Almacén de datos.Asignar espacio** en el almacén de datos de destino.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Seleccione **Menú > Bibliotecas de contenido**.

3 Haga clic en **Crear**.

Se abrirá el asistente **Nueva biblioteca de contenido**.

4 Especifique **Nombre y ubicación** de la biblioteca de contenido y haga clic en **Siguiente** cuando haya terminado.

Campo	Descripción
Nombre	Introduzca un nombre descriptivo, como `TanzuKubernetesRelease-subscriber`.
Notas	Incluya una descripción, como `Biblioteca de suscripción a petición de versiones de Tanzu Kubernetes`.
vCenter Server	Seleccione la instancia de vCenter Server en la que vSphere with Tanzu está habilitado.

5 Configure la suscripción de la biblioteca de contenido en la página **Configurar biblioteca de contenido** y haga clic en **Siguiente** cuando haya terminado.

a Seleccione la opción **Biblioteca de contenido suscrita**.

Nota Para utilizar una biblioteca de contenido local, consulte Crear, proteger y sincronizar una biblioteca de contenido local para versiones de Tanzu Kubernetes.

b Introduzca la dirección **URL de suscripción** del publicador:

https://wp-content.vmware.com/v2/latest/lib.json

c Para la opción **Descargar contenido**, seleccione una de las siguientes opciones:

Opción	Descripción
Inmediatamente	El proceso de suscripción sincroniza tanto los metadatos como las imágenes de la biblioteca. Si se eliminan elementos de la biblioteca publicada, su contenido se conserva en el almacenamiento de la biblioteca suscrita, por lo que deberá eliminarlo de forma manual.
Cuando sea necesario	El proceso de suscripción sincroniza solo los metadatos de la biblioteca. El servicio Tanzu Kubernetes Grid descarga las imágenes cuando se publican. Cuando ya no necesita el elemento, puede eliminar el contenido del elemento para liberar espacio de almacenamiento. Para ahorrar almacenamiento, se recomienda esta opción.

6 Cuando se le pida, acepte la huella digital del certificado SSL.

El certificado SSL se almacena en su sistema hasta que la biblioteca de contenido suscrita se elimine del inventario.

7 Configure la directiva de seguridad de OVF en la página **Aplicar directiva de seguridad** y haga clic en **Siguiente** cuando haya terminado.

a Seleccione **Aplicar directiva de seguridad**

b Seleccione la **directiva predeterminada de OVF**

Al seleccionar esta opción, el sistema comprueba el certificado de firma de OVF durante el proceso de sincronización. Una plantilla de OVF que no supera la validación del certificado se marca con la etiqueta de **error en la verificación**. Los metadatos de la plantilla se conservan, pero los archivos OVF no se pueden sincronizar.

Nota Actualmente, la **directiva predeterminada de OVF** es la única directiva de seguridad compatible.

---

8 En la página **Agregar almacenamiento**, seleccione un almacén de datos como ubicación de almacenamiento para el contenido de la biblioteca de contenido y haga clic en **Siguiente**.

9 En la página **Listo para completar**, revise los detalles y haga clic en **Finalizar**.

10 En la página **Bibliotecas de contenido**, seleccione la nueva biblioteca de contenido que creó.

11 Confirme o complete la sincronización del contenido de la biblioteca.

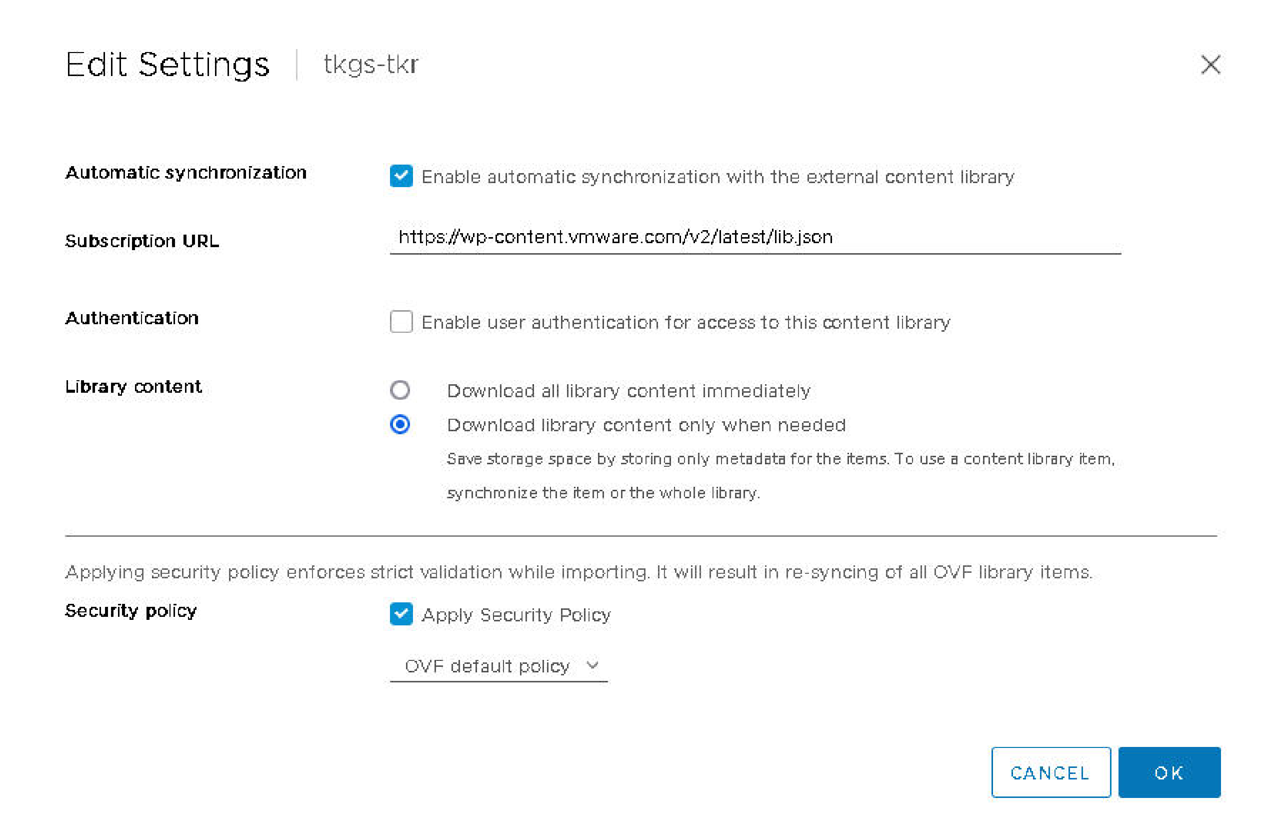
Opción de sincronización	Descripción
Inmediatamente	Si eligió descargar todo el contenido inmediatamente, confirme que la biblioteca está sincronizada. Para ver el contenido de la biblioteca sincronizada, seleccione **Plantillas > Plantillas de OVF y OVA**.
Cuando sea necesario	Si optó por sincronizar la biblioteca a petición, tiene dos opciones: ■ Utilizar **Acciones** > **Sincronizar** toda la biblioteca ■ Hacer clic con el botón secundario en un elemento y seleccionar **Sincronizar** para sincronizar solo eso Para ver el contenido de la biblioteca sincronizada, seleccione **Plantillas > Plantillas de OVF y OVA**.

12 Si eligió la opción **Cuando sea necesario**, descargue las plantillas de OVF que desee utilizar.

Si eligió la opción **Cuando sea necesario**, verá que los archivos de imagen no se almacenan localmente, sino que solo se almacenan los metadatos. Para descargar los archivos de plantilla, seleccione el elemento, haga clic con el botón secundario y seleccione **Sincronizar elemento**.

13 Para actualizar la configuración de la biblioteca de contenido suscrita, seleccione **Acciones > Editar configuración**.

Configuración	Valor
URL de suscripción	https://wp-content.vmware.com/v2/latest/lib.json
Autenticación	No habilitado
Biblioteca de contenido	Descargar cuando sea necesario
directiva de seguridad	Directiva predeterminada de OVF



Pasos siguientes

Configure cada espacio de nombres de vSphere donde aprovisionará los clústeres de Tanzu Kubernetes asociando la biblioteca de contenido y las clases de máquinas virtuales con el espacio de nombres. Consulte Configurar un espacio de nombres de vSphere para las versiones de Tanzu Kubernetes.

Crear, proteger y sincronizar una biblioteca de contenido local para versiones de Tanzu Kubernetes

Para aprovisionar un clúster de Tanzu Kubernetes en un entorno de Internet restringido ("aislado"), cree una biblioteca de contenido local e importe manualmente cada versión de Tanzu Kubernetes.

La creación de una biblioteca de contenido local implica configurar la biblioteca, descargar los archivos OVA e importarlos a la biblioteca de contenido local.

Requisitos previos

Revise Acerca de las distribuciones de versión de Tanzu Kubernetes.

Se requieren los siguientes privilegios para crear una biblioteca de contenido suscrita:

- **Biblioteca de contenido.Crear biblioteca local** o **Biblioteca de contenido.Crear biblioteca suscrita** en la instancia de vCenter Server en la que desea crear la biblioteca.
- **Almacén de datos.Asignar espacio** en el almacén de datos de destino.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Haga clic en **Menú**.

3 Haga clic en **Biblioteca de contenido**.

4 Haga clic en **Crear**.

El sistema muestra el asistente **Nueva biblioteca de contenido**.

5 Especifique **Nombre y ubicación** de la biblioteca de contenido y haga clic en **Siguiente** cuando haya terminado.

Campo	Descripción
Nombre	Introduzca un nombre descriptivo, como **TanzuKubernetesRelease-local**.
Notas	Incluya una descripción, como **Biblioteca local para versiones de Tanzu Kubernetes**.
vCenter Server	Seleccione la instancia de vCenter Server en la que vSphere with Tanzu está habilitado.

6 En la página **Configurar biblioteca de contenido**, seleccione la opción **Biblioteca de contenido local** y haga clic en **Siguiente**.

Como se describe a continuación, para las bibliotecas de contenido locales, importe manualmente las plantillas de OVF que desee utilizar.

Nota Para utilizar una biblioteca de contenido suscrita, consulte Crear, proteger y sincronizar una biblioteca de contenido suscrita para las versiones de Tanzu Kubernetes.

7 Configure la directiva de seguridad de OVF en la página **Aplicar directiva de seguridad** y haga clic en **Siguiente** cuando haya terminado.

a Seleccione **Aplicar directiva de seguridad**

b Seleccione la **directiva predeterminada de OVF**

Al seleccionar esta opción, el sistema comprueba el certificado de firma de OVF durante el proceso de sincronización. Una plantilla de OVF que no supera la validación del certificado se marca con la etiqueta de **error en la verificación**. Los metadatos de la plantilla se conservan, pero los archivos OVF no se pueden sincronizar.

Nota Actualmente, la **directiva predeterminada de OVF** es la única directiva de seguridad compatible.

8 En la página **Agregar almacenamiento**, seleccione un almacén de datos como ubicación de almacenamiento para el contenido de la biblioteca de contenido y haga clic en **Siguiente**.

9 En la página **Listo para completar**, revise los detalles y haga clic en **Finalizar**.

10 En la página **Bibliotecas de contenido**, seleccione la nueva biblioteca de contenido que creó.

11 Descargue los archivos OVA de cada versión de Tanzu Kubernetes que desee importar a la biblioteca de contenido local.

   a Visite la siguiente URL en un navegador:

      https://wp-content.vmware.com/v2/latest/

   b Haga clic en el directorio de la imagen que desee. Por lo general, este directorio es la última versión o la más reciente de la distribución de Kubernetes.

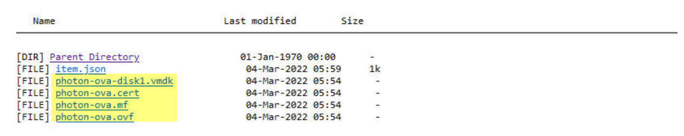
      Por ejemplo:

```
ob-18186591-photon-3-k8s-v1.20.7---vmware.1-tkg.1.7fb9067
```

      Nota El nombre de la distribución es necesario para importar los archivos a la biblioteca de contenido local, por lo que es posible que desee copiarlo en un archivo o mantener el explorador abierto hasta que complete el procedimiento.

   c Para cada uno de los siguientes archivos, haga clic con el botón secundario y seleccione **Guardar vínculo como**.

      - `photon-ova-disk1.vmdk`
      - `photon-ova.cert`
      - `photon-ova.mf`
      - `photon-ova.ovf`



   d Compruebe que cada archivo se descarga correctamente en el sistema de archivos local.

   Nota Si el archivo de manifiesto y el certificado no están disponibles en el directorio de origen durante el proceso de importación, el elemento de la biblioteca importado no podrá usarse. Esto significa que, para una biblioteca de contenido local configurada con una directiva de seguridad, los cuatro archivos necesarios deben estar en el directorio local desde el que se importan los archivos ovf y vmdk. Además de los archivos ovf y vmdk, también debe descargar los archivos de certificado y manifiesto y colocar los cuatro archivos en el mismo directorio de origen.

12 Importe los archivos OVA descargados a la biblioteca de contenido local.

   a Seleccione **Menú > Bibliotecas de contenido >** .

   b En la lista de **Bibliotecas de contenido**, haga clic en el vínculo del nombre de la biblioteca de contenido local que haya creado.

   c Haga clic en **Acciones**.

d Seleccione **Importar elemento**.

e En la ventana **Importar elemento de biblioteca**, seleccione **Archivo local**.

f Haga clic en **Cargar archivos**.

g Seleccione los archivos `photon-ova.ovf` y `photon-ova-disk1.vmdk`.

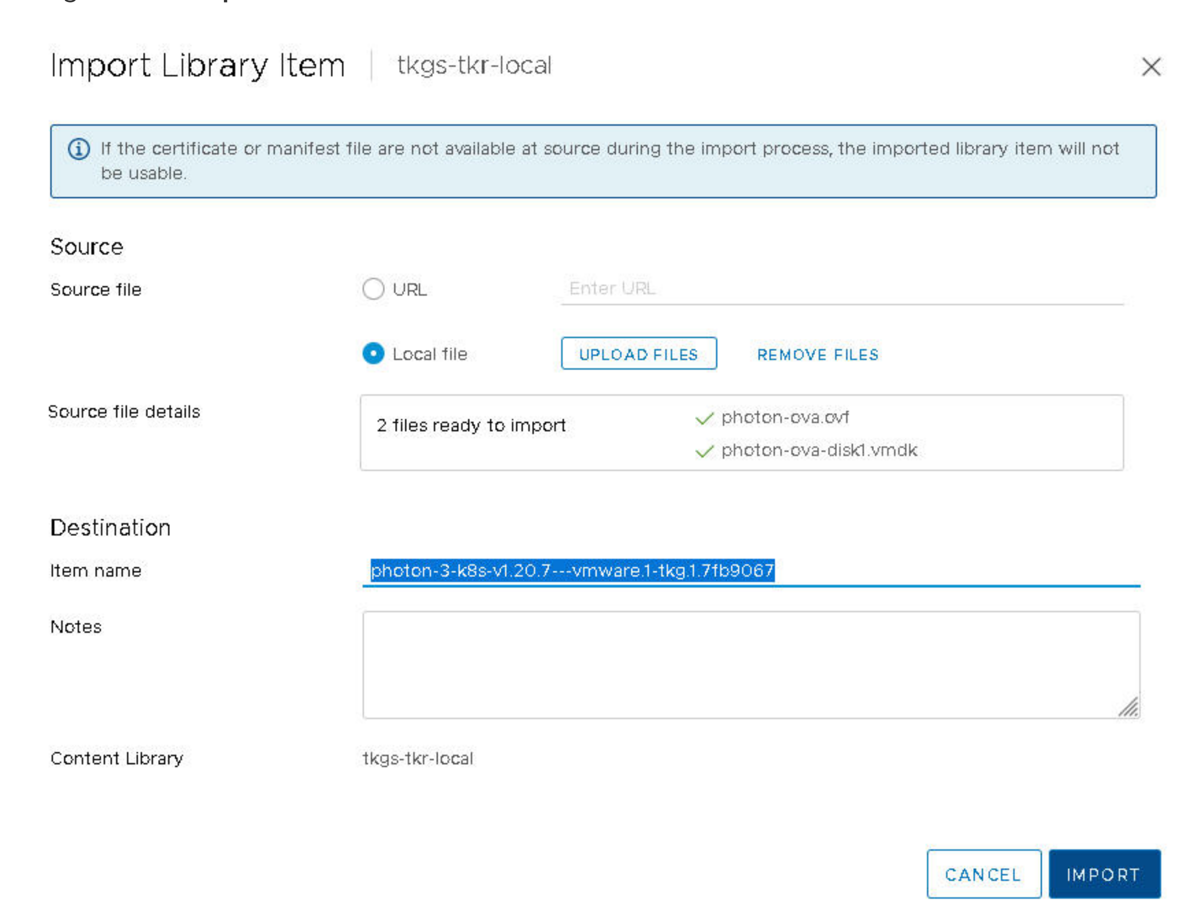
Verá el mensaje `2 files ready to import`. Cada archivo se muestra con una marca de verificación de color verde junto a su nombre.

h Cambie el nombre del **Elemento de destino** de manera que indique la versión de la imagen de Photon más la versión de Kubernetes desde el directorio donde descargó los archivos.

Por ejemplo:

```
photon-3-k8s-v1.20.7---vmware.1-tkg.1.7fb9067
```

i Haga clic en **Importar**.



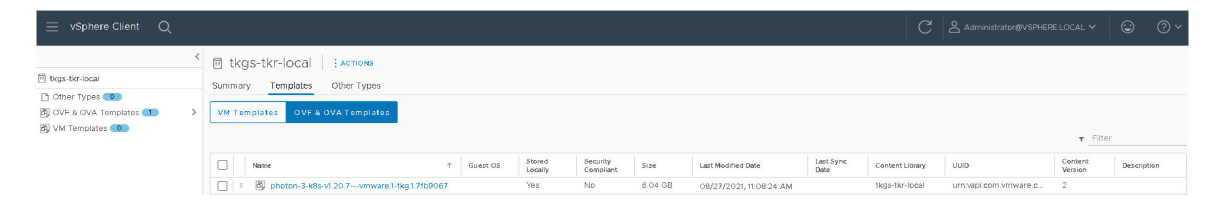
13 Compruebe que se haya rellenado la biblioteca de contenido local con la versión de Tanzu Kubernetes.

   a Despliegue el panel **Tareas recientes** en la parte inferior de la página.

   b Supervise la tarea **Obtener contenido de un elemento de biblioteca** y compruebe que se haya **Completado** correctamente.

   c En la biblioteca de contenido local, seleccione **Plantillas > Plantillas de OVF y OVA**.

   d Compruebe que los metadatos de la versión de Tanzu Kubernetes aparecen en la lista y que su contenido se almacena localmente.



Pasos siguientes

Configure cada espacio de nombres de vSphere donde aprovisionará los clústeres de Tanzu Kubernetes asociando la biblioteca de contenido y las clases de máquinas virtuales con el espacio de nombres. Consulte Configurar un espacio de nombres de vSphere para las versiones de Tanzu Kubernetes.

Migrar clústeres de Tanzu Kubernetes a una nueva biblioteca de contenido

Si la biblioteca de contenido suscrita alcanza la capacidad, puede migrar un clúster de Tanzu Kubernetes para utilizar una biblioteca nueva con capacidad de almacenamiento adicional.

Cuando el administrador de vSphere crea una biblioteca de contenido suscrita, el administrador especifica un almacén de datos donde se almacenará el contenido de la biblioteca que, en este caso, son archivos OVA. Con el paso del tiempo, a medida que se distribuyan más versiones de Kubernetes, la biblioteca de contenido suscrita se expandirá conforme se vayan agregando archivos OVA para cada actualización. Si bien no hay capacidad explícita en la biblioteca de contenido suscrita, estará limitará por su capacidad de almacén de datos.

Si la biblioteca de contenido suscrita alcanza su capacidad, es posible que aparezca el mensaje `Internal error occurred: get library items failed for.` En ese caso, puede migrar el clúster de Tanzu Kubernetes a una nueva biblioteca de contenido suscrita para aumentar la capacidad de almacenamiento. La migración la realizaría un administrador de vSphere mediante vSphere Client.

Procedimiento

1 Cree una nueva biblioteca de contenido suscrita con capacidad suficiente para el clúster de destino. Consulte Crear, proteger y sincronizar una biblioteca de contenido suscrita para las versiones de Tanzu Kubernetes.

2 Inicie sesión en vCenter Server mediante vSphere Client.

3 Seleccione **Menú > Hosts y clústeres**.

4 Seleccione el objeto de clúster de vSphere en el que se aprovisiona la instancia de clúster supervisor que contiene el clúster de Tanzu Kubernetes.

5 Seleccione la pestaña **Configurar**.

6 Seleccione la opción **Espacios de nombres > General >** en el panel de navegación.

7 Haga clic en **Editar** junto a la sección **Biblioteca de contenido** del panel principal.

8 Seleccione la nueva biblioteca de contenido que creó y haga clic en **Aceptar**.

Esta acción activa la actualización de la configuración del clúster.

Nota Después de modificar la biblioteca de contenido, el clúster de Tanzu Kubernetes podría tardar hasta 10 minutos en seleccionar el cambio del origen de contenido.

Importar el archivo OVA de HAProxy a una biblioteca de contenido local

Si utiliza redes de vDS, le puede convenir importar el archivo OVA de HAProxy a una biblioteca de contenido. La importación de archivos OVA de HAProxy a una biblioteca de contenido local se puede utilizar en implementaciones aisladas.

Requisitos previos

Cree una biblioteca de contenido local. Consulte Crear, proteger y sincronizar una biblioteca de contenido local para versiones de Tanzu Kubernetes.

Descargue la versión más reciente del archivo OVA de VMware HAProxy desde el sitio de VMware-HAProxy.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Seleccione **Menú > Bibliotecas de contenido >** .

3 En la lista de **Bibliotecas de contenido**, haga clic en el vínculo del nombre de la biblioteca de contenido local que haya creado; por ejemplo, **HAProxy**.

4 Haga clic en **Acciones**.

5 Seleccione **Importar elemento**.

6 En la ventana **Importar elemento de biblioteca**, seleccione **Archivo local**.

7 Haga clic en **Cargar archivos**.

8 Seleccione el archivo `vmware-haproxy-vX.X.X.ova`.

Verá el mensaje `1 file ready to import`. El archivo aparece con una marca de verificación de color verde junto a su nombre.

9 Haga clic en **Importar**.

10 Despliegue el panel **Tareas recientes** en la parte inferior de la página.

11 Supervise la tarea **Obtener contenido de un elemento de biblioteca** y compruebe que se haya **Completado** correctamente.

Pasos siguientes

Implemente la máquina virtual del plano de control de HAProxy. Consulte Implementar la máquina virtual del plano de control del equilibrador de carga de HAProxy.

Crear y administrar bibliotecas de contenido para máquinas virtuales independientes en vSphere with Tanzu

Una máquina virtual independiente en el entorno de vSphere with Tanzu requiere acceso a imágenes de máquina virtual, o plantillas, que contienen configuraciones de software, incluidos sistemas operativos, aplicaciones y datos. Para proporcionar acceso a imágenes, configure una biblioteca de contenido de máquina virtual y asóciela con el espacio de nombres donde se implementan las máquinas virtuales.

Procedimiento

1 Crear una biblioteca de contenido para máquinas virtuales independientes en vSphere with Tanzu

   Para implementar máquinas virtuales en el entorno de vSphere with Tanzu, los usuarios de desarrollo y operaciones deben tener acceso a las imágenes y las plantillas de máquina virtual. Como administrador de vSphere, cree una biblioteca de contenido para almacenar y administrar plantillas de máquina virtual.

2 Rellenar una biblioteca de contenido con imágenes de máquina virtual para máquinas virtuales independientes en vSphere with Tanzu

   Como administrador de vSphere, rellene una biblioteca de contenido con plantillas de máquina virtual en formato OVA u OVF. Los ingenieros de desarrollo y operaciones pueden utilizar las plantillas para aprovisionar nuevas máquinas virtuales independientes en el entorno de vSphere with Tanzu.

3 Asociar una biblioteca de contenido de máquina virtual con un espacio de nombres en vSphere with Tanzu

   Como administrador de vSphere, debe proporcionar su usuario de acceso de desarrollo y operaciones a un origen de plantillas de máquina virtual, de modo que los ingenieros de desarrollo y operaciones puedan utilizar las plantillas para aprovisionar nuevas máquinas virtuales independientes en el entorno de vSphere with Tanzu. Para proporcionar acceso, agregue una biblioteca de contenido con plantillas de máquina virtual al espacio de nombres.

4 Administrar bibliotecas de contenido de máquina virtual en un espacio de nombres en vSphere with Tanzu

Como administrador de vSphere, debe asociar una biblioteca de contenido que contiene plantillas de máquina virtual con un espacio de nombres, de modo que los ingenieros de desarrollo y operaciones puedan utilizar las plantillas para aprovisionar máquinas virtuales independientes en el entorno de vSphere with Tanzu. Después de asociar la biblioteca con el espacio de nombres, puede eliminar la biblioteca para anular su publicación del espacio de nombres de Kubernetes. También puede agregar más bibliotecas.

Crear una biblioteca de contenido para máquinas virtuales independientes en vSphere with Tanzu

Para implementar máquinas virtuales en el entorno de vSphere with Tanzu, los usuarios de desarrollo y operaciones deben tener acceso a las imágenes y las plantillas de máquina virtual. Como administrador de vSphere, cree una biblioteca de contenido para almacenar y administrar plantillas de máquina virtual.

Puede crear una biblioteca de contenido local y rellenarla con plantillas y otros tipos de archivos.

También puede crear una biblioteca suscrita para utilizar el contenido de una biblioteca local publicada ya existente.

A partir de vSphere 7.0 Update 3, puede proteger los elementos de una biblioteca de contenido mediante la aplicación de una directiva de seguridad de OVF. La directiva de seguridad de OVF aplica una validación estricta al implementar o actualizar una biblioteca de contenido, importar elementos a una biblioteca de contenido o sincronizar plantillas. Para asegurarse de que las plantillas estén firmadas por un certificado de confianza, puede agregar el certificado de firma de OVF desde una entidad de certificación de confianza en una biblioteca de contenido.

Para obtener más información sobre las bibliotecas de contenido y las plantillas de máquina virtual de vSphere, consulte Usar bibliotecas de contenido.

Requisitos previos

Privilegios necesarios:

- **Biblioteca de contenido.Crear biblioteca local** o **Biblioteca de contenido.Crear biblioteca suscrita** en la instancia de vCenter Server en la que desea crear la biblioteca.
- **Almacén de datos.Asignar espacio** en el almacén de datos de destino.

Procedimiento

1 Desplácese a la página **Servicio de máquina virtual**.

   a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

   b Haga clic en la pestaña **Servicios** y haga clic en **Administrar** en el panel **Servicio de máquina virtual**.

2 En la página **Servicio de máquina virtual**, haga clic en **Bibliotecas de contenido > Crear una biblioteca de contenido**.

Esta acción lo lleva a la sección de la biblioteca de contenido de vSphere Client.

3 Haga clic en **Crear**.

Se abrirá el asistente **Nueva biblioteca de contenido**.

4 En la página **Nombre y ubicación**, introduzca un nombre, seleccione una instancia de vCenter Server para la biblioteca de contenido y haga clic en **Siguiente**.

Asegúrese de utilizar un nombre informativo para la biblioteca de contenido, de modo que el equipo de desarrollo y operaciones pueda encontrarlos y acceder a ellos fácilmente.

5 En la página **Configurar biblioteca de contenido**, seleccione el tipo de biblioteca de contenido que desea crear y haga clic en **Siguiente**.

Opción	Descripción
Biblioteca de contenido local	De forma predeterminada, solo se puede acceder a una biblioteca de contenido local en la instancia de vCenter Server en la que se creó. a (opcional) Para que el contenido de la biblioteca esté disponible para otras instancias de vCenter Server, seleccione **Habilitar publicación**. b (opcional) Si desea requerir una contraseña para acceder a la biblioteca de contenido, seleccione **Permitir autenticación** y establezca una contraseña.
Biblioteca de contenido suscrita	Una biblioteca de contenido suscrita se origina en una biblioteca de contenido publicada. Utilice esta opción para aprovechar las bibliotecas de contenido existentes. Es posible sincronizar la biblioteca suscrita con la biblioteca publicada para ver el contenido actualizado, pero no se puede agregar ni quitar contenido de la biblioteca suscrita. Solo un administrador de la biblioteca publicada puede agregar, modificar y quitar contenido de la biblioteca publicada. Proporcione la siguiente información para suscribirse a una biblioteca: a En el cuadro de texto **URL de suscripción**, escriba la dirección URL de la biblioteca publicada. b Si está habilitada la autenticación en la biblioteca publicada, seleccione **Habilitar autenticación** y escriba la contraseña del editor. c Seleccione un método de descarga para el contenido de la biblioteca suscrita. ■ Si desea descargar una copia local de todos los elementos de una biblioteca publicada inmediatamente después de suscribirla, seleccione **inmediatamente**. ■ Si desea ahorrar espacio de almacenamiento, seleccione **solo cuando sea necesario**. Solo se descargan los metadatos para los elementos de la biblioteca publicada. Si necesita utilizar un elemento, sincronice el elemento o la biblioteca completa para descargar su contenido. d Cuando se le pida, acepte la huella digital de certificado SSL. El certificado SSL se almacena en su sistema hasta que la biblioteca de contenido suscrita se elimine del inventario.

6 (opcional) En la página **Aplicar directiva de seguridad**, seleccione **Aplicar directiva de seguridad** y seleccione **Directiva predeterminada de OVF**.

   Para la biblioteca suscrita, esta opción aparece solo si la biblioteca admite políticas de seguridad.

   Si selecciona esta opción, el sistema realiza una verificación de certificado OVF estricta al importar un elemento de OVF a la biblioteca desde el host local o sincronizar un elemento. No se pueden importar los elementos de OVF que no aprueben la validación del certificado.

   Si el elemento no supera la validación durante la sincronización, se marca con la etiqueta **Error en la verificación**. Solo se conservarán el elemento y los metadatos, pero no los archivos del elemento.

7 En la página **Agregar almacenamiento**, seleccione un almacén de datos como ubicación de almacenamiento para el contenido de la biblioteca de contenido y haga clic en **Siguiente**.

8 En la página **Listo para completar**, revise los detalles y haga clic en **Finalizar**.

Pasos siguientes

Después de crear la biblioteca de contenido, rellene la biblioteca con plantillas de máquina virtual para que los ingenieros de desarrollo y operaciones puedan usar las plantillas para aprovisionar nuevas máquinas virtuales. Consulte Rellenar una biblioteca de contenido con imágenes de máquina virtual para máquinas virtuales independientes en vSphere with Tanzu.

Rellenar una biblioteca de contenido con imágenes de máquina virtual para máquinas virtuales independientes en vSphere with Tanzu

Como administrador de vSphere, rellene una biblioteca de contenido con plantillas de máquina virtual en formato OVA u OVF. Los ingenieros de desarrollo y operaciones pueden utilizar las plantillas para aprovisionar nuevas máquinas virtuales independientes en el entorno de vSphere with Tanzu.

Después de crear una biblioteca de contenido, puede rellenarla con elementos de varias maneras. En este tema se describe cómo puede agregar elementos a una biblioteca de contenido local mediante la importación de archivos del equipo local o desde un servidor web. Para obtener otras maneras de rellenar la biblioteca de contenido, consulte Rellenar bibliotecas con contenido.

Requisitos previos

- Cree una biblioteca de contenido para el aprovisionamiento de máquinas virtuales. Crear una biblioteca de contenido para máquinas virtuales independientes en vSphere with Tanzu.
- Use solo imágenes de máquina virtual compatibles que aparezcan en VMware Cloud Marketplace como OVF. Para buscar imágenes compatibles, busque la **`imagen del servicio de máquina virtual`** en el sitio web VMware Cloud Marketplace. Vea un ejemplo de la imagen del servicio de máquina virtual para CentOS en Imagen de servicio de máquina virtual para CentOS.

- Si la biblioteca está protegida por una directiva de seguridad, asegúrese de que todos los elementos de la biblioteca sean compatibles. Si una biblioteca protegida incluye una combinación de elementos conformes y no conformes, `kubectl get virtualmachineimages` no puede presentar imágenes de máquina virtual a los ingenieros de desarrollo y operaciones.
- Privilegio necesario: **Biblioteca de contenido.Agregar elemento de biblioteca** y **Biblioteca de contenido.Actualizar archivos** en la biblioteca.

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Bibliotecas de contenido**.

2 Haga clic con el botón derecho en una biblioteca de contenido local y seleccione **Importar elemento**.

Se abrirá el cuadro de diálogo **Importar elemento de la biblioteca**.

3 En la sección **Origen**, seleccione el origen del elemento.

Opción	Descripción
URL	Introduzca la ruta de acceso al servidor web donde se encuentra el elemento. **Nota** Puede importar un archivo `.ovf` o `.ova`. El elemento de biblioteca de contenido resultante es del tipo de plantilla de OVF.
Archivo local	Haga clic en **Cargar archivo** para desplazarse hasta el archivo que desea importar desde el sistema local. Puede utilizar el menú desplegable para filtrar los archivos en el sistema local. **Nota** Puede importar un archivo `.ovf` o `.ova`. Al importar una plantilla de OVF, en primer lugar seleccione el archivo de descriptor OVF (`.ovf`). A continuación, se le solicitará que seleccione los demás archivos en la plantilla de OVF (por ejemplo, el archivo `.vmdk`). El elemento de biblioteca de contenido resultante es del tipo de plantilla de OVF.

vCenter Server lee y valida los archivos de manifiesto y de certificado en el paquete de OVF durante la importación. Se muestra una advertencia en el asistente **Elemento de biblioteca de importación** si existen problemas con el certificado, por ejemplo, si vCenter Server detecta un certificado caducado.

Nota vCenter Server no lee el contenido firmado si se importa el paquete de OVF desde un archivo `.ovf` de la máquina local.

4 En la sección **Destino**, introduzca un nombre y una descripción para el elemento.

5 Haga clic en **Importar**.

Resultados

El elemento aparecerá en la pestaña **Plantillas** o en la pestaña **Otros tipos**.

Pasos siguientes

Después de crear la biblioteca de contenido y rellenarla con plantillas de máquina virtual, agregue la biblioteca al espacio de nombres para proporcionar a los usuarios de Desarrollo y operaciones acceso a la biblioteca de contenido. Consulte Asociar una biblioteca de contenido de máquina virtual con un espacio de nombres en vSphere with Tanzu.

Asociar una biblioteca de contenido de máquina virtual con un espacio de nombres en vSphere with Tanzu

Como administrador de vSphere, debe proporcionar su usuario de acceso de desarrollo y operaciones a un origen de plantillas de máquina virtual, de modo que los ingenieros de desarrollo y operaciones puedan utilizar las plantillas para aprovisionar nuevas máquinas virtuales independientes en el entorno de vSphere with Tanzu. Para proporcionar acceso, agregue una biblioteca de contenido con plantillas de máquina virtual al espacio de nombres.

Puede agregar varias bibliotecas de contenido a un único espacio de nombres. Puede agregar la misma biblioteca de contenido a distintos espacios de nombres.

Nota Este procedimiento se aplica solo a las bibliotecas de contenido para el servicio de máquina virtual. Las bibliotecas de contenido de servicio Tanzu Kubernetes Grid deben administrarse desde el panel de servicio Tanzu Kubernetes Grid.

Requisitos previos

- Cree una biblioteca de contenido. Consulte Crear una biblioteca de contenido para máquinas virtuales independientes en vSphere with Tanzu.
- Rellene la biblioteca con plantillas de máquina virtual. Consulte Rellenar una biblioteca de contenido con imágenes de máquina virtual para máquinas virtuales independientes en vSphere with Tanzu.
- Privilegios necesarios:
  - **Espacio de nombres.Modificar configuración de todo el clúster**
  - **Espacio de nombres.Modificar configuración del espacio de nombres**

Procedimiento

1 En vSphere Client, vaya al espacio de nombres.

   a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

   b Haga clic en la pestaña **Espacios de nombres** y haga clic en el espacio de nombres.

2 Agregue una biblioteca de contenido.

   a En el panel **Servicio de máquina virtual**, haga clic en **Agregar biblioteca de contenido**.

   b Seleccione una o varias bibliotecas de contenido y haga clic en **Aceptar**.

Resultados

El contenido de la biblioteca que agregó se vuelve disponible en el espacio de nombres de Kubernetes como imágenes de máquina virtual, y desarrollo y operaciones puede utilizarlo para realizar el autoservicio de las máquinas virtuales. Consulte Implementar una máquina virtual en vSphere with Tanzu.

Pasos siguientes

Después de asociar una biblioteca de contenido con un espacio de nombres, puede agregar más bibliotecas de contenido o eliminar la biblioteca para cancelar su publicación en el espacio de nombres de Kubernetes. Consulte Administrar bibliotecas de contenido de máquina virtual en un espacio de nombres en vSphere with Tanzu.

Administrar bibliotecas de contenido de máquina virtual en un espacio de nombres en vSphere with Tanzu

Como administrador de vSphere, debe asociar una biblioteca de contenido que contiene plantillas de máquina virtual con un espacio de nombres, de modo que los ingenieros de desarrollo y operaciones puedan utilizar las plantillas para aprovisionar máquinas virtuales independientes en el entorno de vSphere with Tanzu. Después de asociar la biblioteca con el espacio de nombres, puede eliminar la biblioteca para anular su publicación del espacio de nombres de Kubernetes. También puede agregar más bibliotecas.

La eliminación de una biblioteca de contenido de un espacio de nombres no afecta a las máquinas virtuales que se implementaron previamente con las imágenes de la biblioteca.

Nota Este procedimiento se aplica solo a las bibliotecas de contenido para el servicio de máquina virtual. Las bibliotecas de contenido de servicio Tanzu Kubernetes Grid deben administrarse desde el panel de servicio Tanzu Kubernetes Grid.

Requisitos previos

- Agregue una biblioteca de contenido a un espacio de nombres. Asociar una biblioteca de contenido de máquina virtual con un espacio de nombres en vSphere with Tanzu.
- Privilegios necesarios:
  - **Espacio de nombres.Modificar configuración de todo el clúster**
  - **Espacio de nombres.Modificar configuración del espacio de nombres**

Procedimiento

1 En vSphere Client, vaya al espacio de nombres.

   a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

   b Haga clic en la pestaña **Espacios de nombres** y haga clic en el espacio de nombres.

2 Agregue o elimine una biblioteca de contenido.

   a En el panel **Servicio de máquina virtual**, haga clic en **Administrar biblioteca de contenido**.

   b Realice una de las siguientes operaciones.

Opción	Descripción
Eliminar una biblioteca de contenido	Anule la selección de la biblioteca de contenido y haga clic en **Aceptar**.
Agregar una biblioteca de contenido	Seleccione una o varias bibliotecas de contenido y haga clic en **Aceptar**.

Pasos siguientes

El contenido de la biblioteca se vuelve disponible en el espacio de nombres de Kubernetes como imágenes de máquina virtual, y desarrollo y operaciones puede utilizarlo para realizar el autoservicio de las máquinas virtuales. Consulte Implementar una máquina virtual en vSphere with Tanzu.

Configurar y administrar los espacios de nombres de vSphere

7

Las cargas de trabajo de vSphere with Tanzu, incluidos los pods de vSphere, las máquinas virtuales y los clústeres de Tanzu Kubernetes, se implementan en un espacio de nombres de vSphere. Defina un espacio de nombres de vSphere en un clúster supervisor y configúrelo con una cuota de recursos y permisos de usuario. En función de las necesidades de DevOps y las cargas de trabajo que piensen ejecutar, también puede asignar directivas de almacenamiento, clases de máquina virtual y bibliotecas de contenido para obtener las imágenes de máquina virtual y las versiones de Tanzu Kubernetes más recientes.

Este capítulo incluye los siguientes temas:

- Creación y configuración de un espacio de nombres de vSphere
- Establecer reservas y límites de CPU y de memoria predeterminados para los contenedores de pod de vSphere
- Configurar limitaciones en objetos de Kubernetes en un espacio de nombres de vSphere
- Supervisar y administrar recursos en un espacio de nombres de vSphere
- Configurar un espacio de nombres de vSphere para las versiones de Tanzu Kubernetes
- Agregar directivas de seguridad a un espacio de nombres de clúster supervisor en NSX
- Aprovisionar una plantilla de espacio de nombres de autoservicio

Creación y configuración de un espacio de nombres de vSphere

Como administrador de vSphere, debe crear un espacio de nombres de vSphere en el clúster supervisor. Los límites de recursos se establecen en el espacio de nombres y los permisos para que los ingenieros de desarrollo y operaciones puedan acceder a ellos. Debe proporcionar a los ingenieros de desarrollo y operaciones la dirección URL del plano de control de Kubernetes donde pueden ejecutar cargas de trabajo de Kubernetes en los espacios de nombres para los que tienen permisos.

Los espacios de nombres de clústeres supervisor que se configuran con la pila de redes de vSphere y los espacios de nombres de los clústeres configurados con NSX-T Data Center tienen diferentes capacidades y configuración de redes.

Los espacios de nombres que se crean en los clústeres supervisor configurados con NSX-T Data Center admiten el conjunto completo de capacidades de la plataforma de administración de cargas de trabajo. Admiten pods de vSphere, máquinas virtuales y clústeres de Tanzu Kubernetes. NSX-T Data Center proporciona la compatibilidad con redes de cargas de trabajo para estos espacios de nombres. Para obtener más información, consulte Requisitos del sistema para configurar vSphere with Tanzu con NSX-T Data Center.

Los espacios de nombres que se crean en un clúster supervisor configurado con la pila de redes de vSphere solo admiten máquinas virtuales y clústeres de Tanzu Kubernetes; no admiten pods de vSphere y no permiten que se use el registro de Harbor con ellos. La instancia de vSphere Distributed Switch que está conectada a los hosts que forman parte de clúster supervisor proporciona la compatibilidad de redes de cargas de trabajo para estos espacios de nombres. Para obtener más información, consulte Requisitos del sistema para configurar vSphere with Tanzu con redes de vSphere y el equilibrador de carga de HAProxy.

También puede establecer límites de recursos para el espacio de nombres, asignar permisos y aprovisionar o activar el servicio de espacio de nombres en un clúster como una plantilla. Como resultado, los ingenieros de desarrollo y operaciones pueden crear un espacio de nombres de supervisor de autoservicio e implementar cargas de trabajo dentro de él. Para obtener más información, consulte Aprovisionar una plantilla de espacio de nombres de autoservicio.

Requisitos previos

- Configure un clúster con vSphere with Tanzu.
- Cree usuarios o grupos para todos los ingenieros de desarrollo y operaciones que tendrán acceso al espacio de nombres.
- Cree directivas de almacenamiento para el almacenamiento persistente. Las directivas de almacenamiento pueden definir diferentes tipos y clases de almacenamiento como, por ejemplo, Oro, Plata y Bronce.
- Cree clases de máquina virtual y bibliotecas de contenido para máquinas virtuales independientes.
- Cree una biblioteca de contenido para versiones de Tanzu Kubernetes para usarla con clústeres de Tanzu Kubernetes. Consulte Crear y administrar bibliotecas de contenido para versiones de Tanzu Kubernetes.
- Privilegios necesarios:
  - **Espacio de nombres.Modificar configuración de todo el clúster**
  - **Espacio de nombres.Modificar configuración del espacio de nombres**

Procedimiento

1. En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.
2. Seleccione la pestaña **Espacios de nombres**.
3. Haga clic en **Crear espacio de nombres**.

4 Seleccione el clúster supervisor donde quiere ubicar el espacio de nombres.

5 Introduzca un nombre para el espacio de nombres.

El nombre debe tener un formato compatible con DNS.

6 En el menú desplegable **Red**, seleccione una red de cargas de trabajo para el espacio de nombres.

Nota Este paso solo está disponible si se crea el espacio de nombres en un clúster que se haya configurado con la pila de redes de vSphere.

7 Si configuró la pila de redes de NSX-T Data Center para el clúster, puede seleccionar **Anular configuración de red del clúster** para anular la configuración de red del clúster y configurar los ajustes de red para el espacio de nombres.

Configure los siguientes ajustes de red para el espacio de nombres:

Opción	Descripción
Modo NAT	El modo NAT está seleccionado de forma predeterminada. Si anula la selección de esta opción, todas las cargas de trabajo, como las direcciones IP del nodo de pods de vSphere, máquinas virtuales y clústeres de Tanzu Kubernetes, son accesibles directamente desde fuera de la puerta de enlace de nivel 0 y no es necesario configurar los CIDR de salida. **Nota** Una vez habilitado el modo de espacio de nombres, no se pueden hacer cambios.
Puerta de enlace de nivel 0	Seleccione la puerta de enlace de nivel 0 que se asociará con la puerta de enlace de nivel 1 del espacio de nombres. Al seleccionar una puerta de enlace de nivel 0, se anula la puerta de enlace de nivel 0 que configuró al habilitar el clúster, por lo que debe volver a configurar los rangos de CIDR. Si selecciona una puerta de enlace VRF vinculada a la puerta de enlace de nivel 0, la red y las subredes se configuran automáticamente. Si seleccionó el modo NAT, debe configurar los CIDR de subred, entrada y salida. Si anula la selección del modo NAT, solo debe configurar la subred y los CIDR de entrada. **Nota** Una vez que se selecciona una puerta de enlace de nivel 0, no se puede cambiar.
CIDR de red de espacio de nombres	Introduzca uno o varios CIDR de IP para crear subredes/segmentos y asignar direcciones IP para cargas de trabajo conectadas a espacios de nombres. **Nota** Introduzca el rango de CIDR si no lo configuró para el clúster. Puede configurar CIDR adicionales después de crear el espacio de nombres editando la configuración de red del espacio de nombres.
Prefijo de subred de espacio de nombres	Introduzca el prefijo de subred que especifica el tamaño de la subred reservada para los segmentos de espacios de nombres. El valor predeterminado es 28. **Nota** Una vez que especifique el prefijo de subred, no podrá cambiarlo.

Opción	Descripción
CIDR de entrada	Introduzca una anotación CIDR que determine el rango de IP de entrada para las direcciones IP virtuales publicadas por el servicio de equilibrador de carga para clústeres de pods de vSphere o Tanzu Kubernetes. Puede configurar CIDR adicionales después de crear el espacio de nombres editando la configuración de red del espacio de nombres.
CIDR de egreso	Introduzca una anotación CIDR que determine el rango de IP de egreso para las direcciones IP SNAT. Puede configurar CIDR adicionales después de crear el espacio de nombres editando la configuración de red del espacio de nombres.
Tamaño del equilibrador de carga	Seleccione el tamaño de la instancia del equilibrador de carga en la puerta de enlace de nivel 1 para el espacio de nombres.

8 Introduzca una descripción y haga clic en **Crear**.

El espacio de nombres se crea en el clúster supervisor.

9 Establezca permisos para que los ingenieros de desarrollo y operaciones puedan acceder al espacio de nombres.

a En el panel **Permisos**, seleccione **Agregar permisos**.

b Seleccione un origen de identidad, un usuario o un grupo, y una función, y haga clic en **Aceptar**.

10 Establezca el almacenamiento persistente en el espacio de nombres.

Las directivas de almacenamiento que se asignan al espacio de nombres controlan cómo se colocan los volúmenes persistentes y los nodos del clúster de Tanzu Kubernetes dentro de los almacenes de datos en el entorno de almacenamiento de vSphere. Las notificaciones de volumen persistente que corresponden a volúmenes persistentes se pueden originar desde una instancia de pod de vSphere o desde la máquina virtual y el clúster de Tanzu Kubernetes. Para obtener más información, consulte Capítulo 10 Usar almacenamiento persistente en vSphere with Tanzu.

a En el panel **Almacenamiento**, seleccione **Agregar almacenamiento**.

b Seleccione una directiva de almacenamiento para controlar la ubicación de los almacenes de datos de los volúmenes persistentes y haga clic en **Aceptar**.

Después de asignar la directiva de almacenamiento, vSphere with Tanzu crea una clase de almacenamiento de Kubernetes que coincide en el espacio de nombres de vSphere. Si utiliza servicio VMware Tanzu™ Kubernetes Grid™, la clase de almacenamiento se replica automáticamente desde el espacio de nombres en el clúster de Kubernetes. Si asigna varias directivas de almacenamiento al espacio de nombres, se crea una clase de almacenamiento independiente para cada directiva de almacenamiento.

11 En el panel Capacidad y uso, seleccione **Editar límites** y configure las limitaciones de recursos en el espacio de nombres.

Opción	Descripción
CPU	La cantidad de recursos de CPU que se reservarán para el espacio de nombres.
Memoria	La cantidad de memoria que se reservará para el espacio de nombres.
Almacenamiento	La cantidad total de espacio de almacenamiento que se reservará para el espacio de nombres.
Límites de directivas de almacenamiento	Establezca la cantidad de almacenamiento dedicado individualmente a cada una de las directivas de almacenamiento que asoció al espacio de nombres.

Se crea un grupo de recursos para el espacio de nombres en vCenter Server. La limitación de almacenamiento determina la cantidad total de almacenamiento disponible para el espacio de nombres, mientras que las directivas de almacenamiento determinan la colocación de los volúmenes persistentes para los pods de vSphere en las clases de almacenamiento asociadas.

12 Configure el servicio de máquina virtual para las máquinas virtuales independientes.

Para obtener información, consulte Capítulo 12 Implementar y administrar máquinas virtuales en vSphere with Tanzu.

13 Configure el espacio de nombres para los clústeres de Tanzu Kubernetes, incluido lo siguiente:

- Asocie la biblioteca de contenido de versión de Tanzu Kubernetes con el espacio de nombres.
- Agregue las clases de máquina virtual predeterminadas al espacio de nombres.

Para obtener más información, consulte Configurar un espacio de nombres de vSphere para las versiones de Tanzu Kubernetes.

Pasos siguientes

Comparta la URL del plano de control de Kubernetes con los ingenieros de desarrollo y operaciones, así como el nombre de usuario que pueden utilizar para iniciar sesión en clúster supervisor a través de Herramientas de la CLI de Kubernetes para vSphere. Puede conceder acceso a más de un espacio de nombres a un ingeniero de desarrollo y operaciones. Consulte Capítulo 9 Conectarse a clústeres de vSphere with Tanzu.

Establecer reservas y límites de CPU y de memoria predeterminados para los contenedores de pod de vSphere

Puede establecer las reservas y los límites de CPU y de memoria predeterminados para los contenedores en un espacio de nombres a través de vSphere Client. Más adelante, los ingenieros de desarrollo y operaciones pueden anular estos valores en las especificaciones del pod que definen. Las solicitudes de contenedor se traducen en las reservas de recursos en los pods de vSphere.

Requisitos previos

- Compruebe que tenga el privilegio **Modificar configuración del espacio de nombres** en clúster supervisor.

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione un espacio de nombres, seleccione **Configurar** y haga clic en **Límites de recursos**

3 Configure los límites y las reservas de CPU y de memoria predeterminados para los contenedores en el espacio de nombres.

Opción	Descripción
Solicitud de CPU	Establezca la reserva de CPU predeterminada para los contenedores en el espacio de nombres.
Límite de la CPU	Establezca el límite predeterminado de uso de CPU para los contenedores en el espacio de nombres.
Solicitud de memoria	Establezca la reserva de memoria predeterminada para los contenedores en el espacio de nombres.
Límite de memoria	Establezca el límite predeterminado para el uso de memoria para los contenedores en el espacio de nombres.

Configurar limitaciones en objetos de Kubernetes en un espacio de nombres de vSphere

Puede configurar limitaciones para los pods que se ejecutan en el espacio de nombres de vSphere, así como limitaciones para diversos objetos de Kubernetes. Las limitaciones que se configuran para un objeto dependen de los detalles de las aplicaciones y del modo en que se desea que consuman los recursos dentro de un espacio de nombres de vSphere.

Requisitos previos

- Compruebe que tenga el privilegio **Modificar configuración del espacio de nombres** en clúster supervisor.

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione el espacio de nombres en el que desea aplicar las restricciones de objeto o contenedor.

3 Para establecer las limitaciones del contenedor, seleccione **Límites de recursos** y haga clic en **Editar**.

Opción	Descripción
Solicitudes de CPU	Establezca la cantidad de solicitudes de CPU para los contenedores.
Límite de la CPU	Establezca la cantidad de CPU que pueden utilizar los contenedores.
Solicitudes de memoria	Establezca la cantidad de solicitudes de memoria para los contenedores.
Límites de memoria	Establezca la cantidad de memoria que pueden utilizar los contenedores.

Nota El impacto del establecimiento de límites de recursos para un espacio de nombres de vSphere en el que se aprovisionan clústeres de Tanzu Kubernetes varía en función del tipo de clase de máquina virtual utilizada para los nodos del clúster. Asegúrese de estar al tanto de las diferencias entre el mejor esfuerzo y el garantizado antes de establecer los límites de recursos. Consulte Clases de máquina virtual para clústeres de Tanzu Kubernetes.

4 Para establecer limitaciones en los objetos de Kubernetes que pueden existir en el espacio de nombres, seleccione **Límites de objetos** y haga clic en **Editar**.

Opción	Descripción
Pods	La cantidad de pod de vSphere que pueden ejecutarse en el espacio de nombres.
Implementaciones	El número de implementaciones que pueden ejecutarse en el espacio de nombres.
Trabajos	La cantidad de trabajos que pueden ejecutarse en el espacio de nombres.
DaemonSets	La cantidad de conjuntos de daemons que pueden ejecutarse en el espacio de nombres.
ReplicaSets	La cantidad de conjuntos de réplicas en el espacio de nombres.
ReplicationControllers	La cantidad de controladoras de replicación que pueden ejecutarse en el espacio de nombres.
StatefulSets	La cantidad de StatefulSets que pueden ejecutarse en el espacio de nombres.
ConfigMaps	La cantidad de ConfigMaps que pueden ejecutarse en el espacio de nombres.
Secretos	La cantidad de secretos que pueden ejecutarse en el espacio de nombres.
Notificaciones de volumen persistente	Las notificaciones de volumen persistente que pueden existir en el espacio de nombres.
Servicios	Los servicios que pueden existir en el espacio de nombres.

Supervisar y administrar recursos en un espacio de nombres de vSphere

Es posible supervisar y administrar diferentes aspectos de un espacio de nombres de vSphere, como el consumo de recursos para el espacio de nombres o la cantidad de objetos de Kubernetes diferentes que existen en un espacio de nombres y que ellos indican.

Requisitos previos

Creación y configuración de un espacio de nombres de vSphere.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Desplácese hasta la vista **Menú > Hosts y clústeres**.

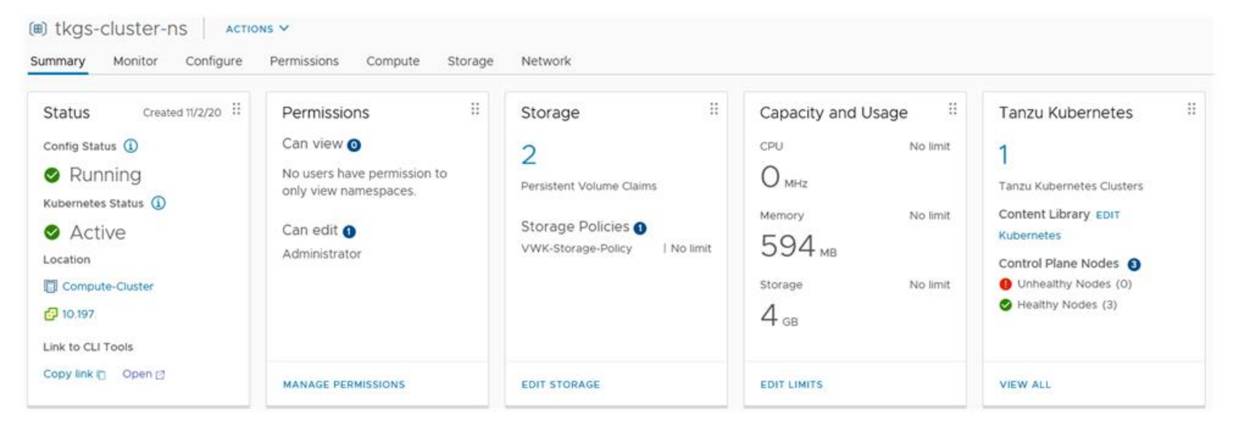
3 Seleccione el clúster de vCenter en el que ha habilitado **Administración de cargas de trabajo**.

4 Seleccione el grupo de recursos de **Espacios de nombres** y expanda su contenido.

   Los nodos del plano de control del clúster supervisor se encuentran en el grupo de recursos de Espacios de nombres. Además, cada espacio de nombres de vSphere que se crea para este clúster supervisor se encuentra en el grupo de recursos **Espacios de nombres**.

5 Seleccione el objeto del espacio de nombres de vSphere, que se representa como un icono de ventana.

   En la pestaña **Resumen**, verá las diferentes secciones de configuración del espacio de nombres de vSphere, incluidas **Estado**, **Permisos**, **Almacenamiento**, **Capacidad y uso** y **Tanzu Kubernetes**. En esta pantalla, puede administrar cualquiera de estos ajustes.



Configurar un espacio de nombres de vSphere para las versiones de Tanzu Kubernetes

Configure el espacio de nombres de vSphere en el que tiene pensado aprovisionar clústeres de Tanzu Kubernetes asociando el espacio de nombres con la biblioteca de contenido para las versiones de Tanzu Kubernetes y con las clases de máquinas virtuales que desea utilizar.

Requisitos previos

Cree un espacio de nombres de vSphere. Consulte Creación y configuración de un espacio de nombres de vSphere.

Cree una biblioteca de contenido para alojar las versiones de Tanzu Kubernetes. Consulte Crear, proteger y sincronizar una biblioteca de contenido suscrita para las versiones de Tanzu Kubernetes o Crear, proteger y sincronizar una biblioteca de contenido local para versiones de Tanzu Kubernetes.

Asociar la biblioteca de contenido con el espacio de nombres de vSphere

Para asociar la biblioteca de contenido creada para las versiones de Tanzu Kubernetes con un espacio de nombres de vSphere, inicie sesión en vCenter Server mediante vSphere Client y complete cualquiera de los siguientes procedimientos.

Asociar mediante la ruta de inventario de vSphere	Asociar mediante la ruta de administración de cargas de trabajo
1 Seleccione **Menú > Hosts y clústeres**. 2 Seleccione el clúster de vSphere en el que está habilitada la **Administración de cargas de trabajo**. 3 Seleccione la pestaña **Configurar**. 4 Seleccione **Espacios de nombres > General**. 5 Seleccione **Configuración del servicio Tanzu Kubernetes Grid**. 6 Haga clic en **Editar** junto a la etiqueta **Biblioteca de contenido**. 7 Seleccione la biblioteca de contenido de las versiones de Tanzu Kubernetes. 8 Haga clic en **Aceptar**.	1 Seleccione **Menú > Administración de cargas de trabajo**. 2 Seleccione la pestaña **Espacios de nombres**. 3 Seleccione el espacio de nombres de vSphere de destino. 4 Busque el mosaico de **Tanzu Kubernetes Grid Service**. 5 Haga clic en **Editar** junto a la etiqueta **Biblioteca de contenido**. 6 Seleccione la biblioteca de contenido de las versiones de Tanzu Kubernetes. 7 Haga clic en **Aceptar**.

Nota Después de asociar la biblioteca de contenido al espacio de nombres de vSphere, pueden pasar unos minutos hasta que las plantillas de la máquina virtual estén disponibles para el aprovisionamiento de los clústeres de Tanzu Kubernetes. Consulte Comprobar la configuración de espacio de nombres de vSphere.

Asociar las clases de máquinas virtuales con el espacio de nombres de vSphere

vSphere with Tanzu proporciona varias clases de máquinas virtuales predeterminadas, y usted puede crear las suyas propias. Consulte Clases de máquina virtual para clústeres de Tanzu Kubernetes.

Para aprovisionar clústeres de Tanzu Kubernetes, debe asociar las clases de máquinas virtuales que desea utilizar con cada espacio de nombres de vSphere donde desea aprovisionar clústeres de Tanzu Kubernetes.

Para asociar las clases de máquinas virtuales predeterminadas con un espacio de nombres de vSphere, inicie sesión en vCenter Server mediante vSphere Client y complete el siguiente procedimiento.

1 Seleccione **Menú > Administración de cargas de trabajo**.

2 Seleccione la pestaña **Espacios de nombres**.

3 Seleccione el espacio de nombres de vSphere de destino donde quiere aprovisionar el clúster de Tanzu Kubernetes.

4 Busque el mosaico de **Servicio de máquina virtual**.

5 Haga clic en el vínculo **Agregar clase de máquina virtual**.

6 Seleccione las clases de máquinas virtuales que desee agregar.

   a Para agregar las clases de máquina virtual predeterminadas, active la casilla del encabezado de la tabla en la página 1 de la lista, desplácese hasta la página 2 y seleccione la casilla de verificación en el encabezado de la tabla de esa página. Compruebe que todas las clases estén seleccionadas.

   b Para crear una clase personalizada, haga clic en **Crear nueva clase de máquina virtual**. Consulte Crear una clase de máquina virtual en vSphere with Tanzu.

7 Haga clic en **Aceptar** para completar esta operación.

8 Confirme que se hayan agregado las clases. El mosaico de **Servicio de máquina virtual** muestra **Administrar clases de máquinas virtuales**.

Nota La biblioteca de contenido a la que se hace referencia en el mosaico de **Servicio de máquina virtual** debe usarse con máquinas virtuales independientes, y no con versiones de Tanzu Kubernetes. Consulte Crear y administrar bibliotecas de contenido para máquinas virtuales independientes en vSphere with Tanzu.

Comprobar la configuración de espacio de nombres de vSphere

Una vez que haya asociado la biblioteca de contenido y las clases de máquinas virtuales con el espacio de nombres de vSphere, inicie sesión en el clúster supervisor y compruebe que cada versión de Tanzu Kubernetes sincronizada y cada clase de máquina virtual seleccionada estén disponibles.

1 Instale Herramientas de la CLI de Kubernetes para vSphere. Consulte Descargar e instalar Herramientas de la CLI de Kubernetes para vSphere.

2 Inicie sesión en el clúster supervisor.

```
kubectl vsphere login --server IP-ADDRESS-SUPERVISOR-CLUSTER --vsphere-username VCENTER-SSO-USERNAME
```

3 Cambie el contexto al espacio de nombres de vSphere de destino.

```
kubectl config use-context SUPERVISOR-NAMESPACE
```

4 Enumere y describa las versiones de Tanzu Kubernetes disponibles.

```
kubectl get tanzukubernetesreleases
```

```
kubectl describe tanzukubernetesreleases
```

5 Enumere las clases de máquinas virtuales disponibles.

```
kubectl get virtualmachineclassbindings
```

Una vez que se configura el espacio de nombres, puede aprovisionar clústeres de Tanzu Kubernetes. Consulte Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS. Si utiliza una biblioteca de contenido local, deberá especificar un OVA que haya cargado en la biblioteca. Consulte Ejemplos del aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1.

Agregar directivas de seguridad a un espacio de nombres de clúster supervisor en NSX

Un clúster supervisor que utiliza redes de NSX admite directivas de seguridad de red configuradas a través de una CRD de directiva de seguridad.

Crear una directiva de seguridad

Como integrante de desarrollo y operaciones, puede configurar el CRD de la directiva de seguridad para aplicar una directiva de seguridad basada en NSX a un espacio de nombres de clúster supervisor. La directiva de seguridad protege el tráfico de los pods de vSphere y las máquinas virtuales. Las máquinas virtuales incluyen nodos de clústeres de TKG y otras máquinas virtuales implementadas en el clúster supervisor.

Requisitos previos

Utilice la versión 3.2 o posterior de NSX.

Procedimiento

1 Cree un CRD de directiva de seguridad.

Para ver los campos que se deben usar y los ejemplos de CRD, consulte la documentación del CRD de directiva de seguridad de operador NSX en GitHub.

2 Acceda al espacio de nombres en el entorno de Kubernetes.

Consulte Obtener y utilizar el contexto del clúster supervisor.

3 Aplique la directiva de seguridad al espacio de nombres.

```
kubectl apply -f policy-name.yaml
```

4 Vea su directiva de seguridad.

a Vea los detalles de la directiva de seguridad.

```
kubectl get securitypolicy policy-name
```

b Vea una descripción de la directiva de seguridad.

```
kubectl describe securitypolicy policy-name
```

Resultados

También puede utilizar la interfaz de usuario de NSX para ver los detalles de la directiva. Para obtener más información, consulte la página *Documentación de VMware NSX*.

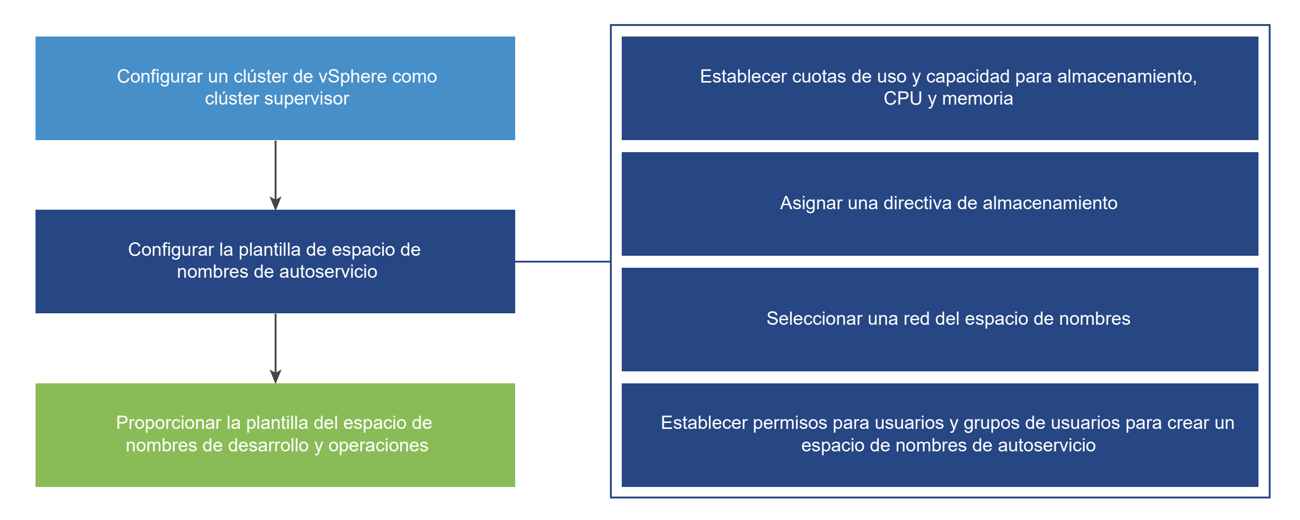
Aprovisionar una plantilla de espacio de nombres de autoservicio

Como administrador de vSphere, puede crear un espacio de nombres de supervisor, establecer límites de CPU, memoria y almacenamiento en el espacio de nombres, asignar permisos y activar el servicio de espacio de nombres en un clúster como una plantilla. Como resultado, los ingenieros de desarrollo y operaciones pueden crear un espacio de nombres de supervisor de autoservicio e implementar cargas de trabajo dentro de él.

Flujo de trabajo de creación y configuración de espacios de nombres de autoservicio

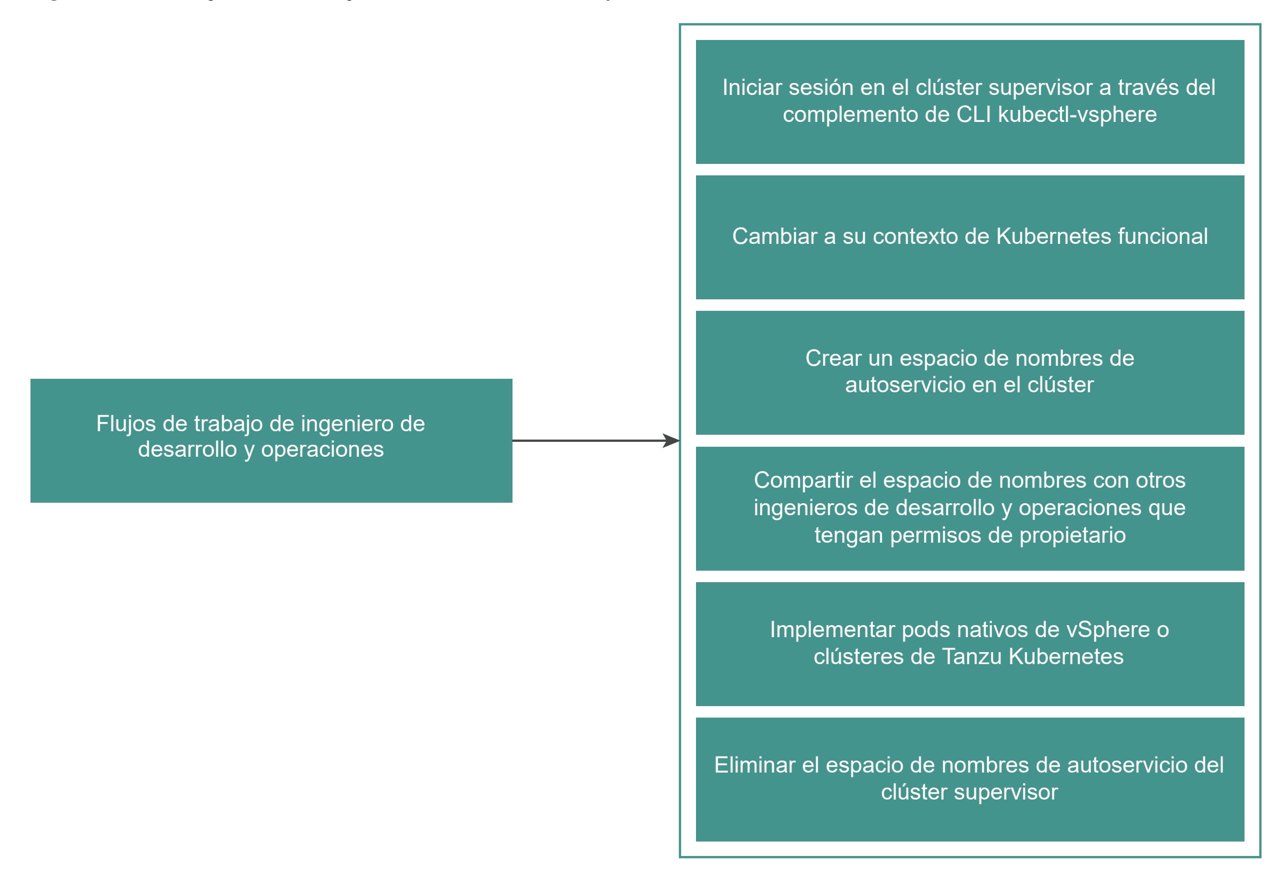
Como administrador de vSphere, puede crear un espacio de nombres de supervisor, establecer límites de CPU, memoria y almacenamiento en el espacio de nombres, asignar permisos y aprovisionar o activar el servicio de espacio de nombres en un clúster como plantilla.

Figura 7-1. Flujo de trabajo de aprovisionamiento de plantilla de espacio de nombres de autoservicio



Como ingeniero de Desarrollo y operaciones, puede crear un espacio de nombres de supervisor mediante autoservicio e implementar cargas de trabajo dentro de él. Puede compartirlo con otros ingenieros de Desarrollo y operaciones, o eliminarlo cuando ya no sea necesario. Para compartir el espacio de nombres con otros ingenieros de desarrollo y operaciones, póngase en contacto con el administrador de vSphere.

Figura 7-2. Flujo de trabajo de creación de espacio de nombres de autoservicio



Crear y configurar una plantilla de espacio de nombres de autoservicio

Como administrador de vSphere, puede crear y configurar un espacio de nombres de supervisor como una plantilla de espacio de nombres de autoservicio. A continuación, los ingenieros de desarrollo y operaciones pueden crear y eliminar espacios de nombres de supervisor mediante la línea de comandos de `kubectl`.

Requisitos previos

Configure un clúster con vSphere with Tanzu.

Procedimiento

1 En vSphere Client, seleccione el clúster de vSphere en el que está habilitado el clúster supervisor.

2 En la pestaña **Configurar**, seleccione **Espacios de nombres > General**.

3 Seleccione **Servicio de espacio de nombres**.

4 Active o desactive el conmutador **Estado** para habilitar la función.

Aparecerá la página **Crear plantilla de espacio de nombres**.

5 En el panel **Configuración**, establezca las limitaciones de recursos para el espacio de nombres.

Opción	Descripción
CPU	La cantidad de recursos de CPU que se reservarán para el espacio de nombres.
Memoria	La cantidad de memoria que se reservará para el espacio de nombres.
Almacenamiento	La cantidad total de espacio de almacenamiento que se reservará para el espacio de nombres.
Directiva de almacenamiento	Establezca la cantidad de almacenamiento dedicado individualmente a cada una de las directivas de almacenamiento que asoció al espacio de nombres.
Red	En el menú desplegable **Red**, seleccione una red para el espacio de nombres.

6 Haga clic en **Siguiente**.

7 En el panel **Permisos**, agregue ingenieros y grupos de desarrollo y operaciones para permitirles utilizar la plantilla con la que pueden crear espacios de nombres.

Seleccione un origen de identidad y un usuario o un grupo, y haga clic en **Siguiente**.

8 En el panel **Revisar y confirmar**, se muestran las propiedades que configura.

Revise las propiedades y haga clic en **Listo**.

Resultados

Se configuró una plantilla de espacio de nombres y tiene estado Activo. Como administrador de vSphere, puede editar la plantilla. Los ingenieros de desarrollo y operaciones pueden utilizar la plantilla para crear espacios de nombres.

Desactivar un espacio de nombres de autoservicio

Como administrador de vSphere, puede desactivar un espacio de nombres de autoservicio en el clúster.

Cuando se desactiva una plantilla de espacio de nombres de autoservicio, los ingenieros de desarrollo y operaciones no pueden usar la plantilla para crear nuevos espacios de nombres en el clúster. Sí pueden eliminar los espacios de nombres que ya crearon.

Procedimiento

1 En vSphere Client, vaya al clúster supervisor.

2 En la pestaña **Configurar**, seleccione **General** en **Espacios de nombres**.

3 En el panel **Autoservicio del espacio de nombres**, alterne el conmutador de **Estado** para desactivar la plantilla.

4 Para volver a activar la plantilla, alterne nuevamente el conmutador de **Estado**.

Puede crear otro espacio de nombres de autoservicio o utilizar el existente.

Crear un espacio de nombres de autoservicio

Como ingeniero de desarrollo y operaciones, puede crear un espacio de nombres de autoservicio y ejecutar cargas de trabajo en él. Una vez creado el espacio de nombres, puede compartirlo con otros ingenieros de desarrollo y operaciones o eliminarlo cuando ya no sea necesario.

Requisitos previos

- Compruebe que un administrador de vSphere haya creado y activado una plantilla de espacio de nombres de autoservicio en el clúster. Consulte Crear y configurar una plantilla de espacio de nombres de autoservicio .
- Compruebe que se haya agregado a la lista de permisos en la plantilla de espacio de nombres de autoservicio de forma individual o como miembro de un grupo.
- Obtenga la dirección IP del plano de control de clúster supervisor.

Procedimiento

1 Utilice complemento de vSphere para kubectl para autenticarse en clúster supervisor. Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

```
kubectl vsphere login --server=IP-ADDRESS --vsphere-username USERNAME
```

2 Cambie el contexto al clúster supervisor.

```
kubectl config use-context SUPERVISOR-CLUSTER-IP
```

3 Cree un espacio de nombres de autoservicio en el clúster.

```
kubectl create namespace NAMESPACE NAME
```

Por ejemplo

```
kubectl create namespace test-ns
```

Nota Los permisos de propietario están disponibles para los ingenieros de desarrollo y operaciones después de habilitar vSphere with Tanzu y actualizar el clúster. Si sólo actualizó vCenter Server y no el clúster, los ingenieros de desarrollo y desarrollo sólo tendrán permisos de edición en los espacios de nombres.

El espacio de nombres que cree aparecerá en el clúster. Para compartir el espacio de nombres con otros ingenieros de desarrollo y operaciones, póngase en contacto con el administrador de vSphere.

Crear un espacio de nombres de autoservicio con anotaciones y etiquetas

Los ingenieros de desarrollo y operaciones pueden crear espacios de nombres de autoservicio con anotaciones y etiquetas mediante la línea de comandos kubectl.

Los ingenieros de desarrollo y operaciones pueden utilizar un manifiesto de YAML con anotaciones y etiquetas definidas por el usuario.

Procedimiento

1 Inicie sesión en el Clúster Supervisor.

   `kubectl vsphere login --server IP-ADDRESS-SUPERVISOR-CLUSTER --vsphere-username VCENTER-SSO-USERNAME`

2 Cree un archivo de manifiesto YAML de espacio de nombres con anotaciones y etiquetas.

   `kubectl create -f ns-create.yaml`

   Por ejemplo, cree el siguiente archivo `ns-create.yaml`:

```
apiVersion: v1
kind: Namespace
metadata:
  name: test-ns-yaml
  labels:
    my-label: "my-label-val-yaml"
  annotations:
    my-ann-yaml: "my-ann-val-yaml"
```

3 Aplique el manifiesto de YAML.

   `kubectl create -f ns-create.yaml`

   O

   `kubectl apply -f ns-create.yaml`

4 Describa el espacio de nombres que creó para ver los cambios.

```
root@localhost [ /tmp ]# kubectl describe ns test-ns-yaml
Name:         test-ns-yaml
Labels:       my-label=my-label-val-yaml
              vSphereClusterID=domain-c50
Annotations:  my-ann-yaml: my-ann-val-yaml
              vmware-system-namespace-owner-count: 1
              vmware-system-resource-pool: resgroup-171
              vmware-system-resource-pool-cpu-limit: 0.4770
              vmware-system-resource-pool-memory-limit: 2000Mi
              vmware-system-self-service-namespace: true
```

```
              vmware-system-vm-folder: group-v172
Status:       Active

Resource Quotas
 Name:             test-ns-yaml
 Resource          Used  Hard
 --------          ---   ---
 requests.storage  0     5000Mi

 Name:                                                                            test-ns-
yaml-storagequota
 Resource                                                                         Used  Hard
 --------                                                                         ---   ---
 namespace-service-storage-profile.storageclass.storage.k8s.io/requests.storage  0
9223372036854775807

No LimitRange resource.
```

Actualizar un espacio de nombres de autoservicio mediante la anotación kubectl y la etiqueta kubectl

El ingeniero de desarrollo y operaciones puede actualizar o eliminar las anotaciones y etiquetas del espacio de nombres de autoservicio mediante los comandos `kubectl annotate` y `kubectl label`.

Requisitos previos

Compruebe que tiene permisos de propietario en el espacio de nombres que desea actualizar.

Procedimiento

1 Inicie sesión en el Clúster Supervisor.

   `kubectl vsphere login --server IP-ADDRESS-SUPERVISOR-CLUSTER --vsphere-username VCENTER-SSO-USERNAME`

2 Describa el espacio de nombres que desea actualizar.

```
root@localhost [ /tmp ]# kubectl describe ns testns
Name:         testns
Labels:       my-label=test-label-2
              vSphereClusterID=domain-c50
Annotations:  my-ann: test-ann-2
              vmware-system-namespace-owner-count: 2
              vmware-system-resource-pool: resgroup-153
              vmware-system-resource-pool-cpu-limit: 0.4770
              vmware-system-resource-pool-memory-limit: 2000Mi
              vmware-system-self-service-namespace: true
              vmware-system-vm-folder: group-v154
Status:       Active


Resource Quotas
 Name:             testns
```

```
 Resource          Used  Hard
 --------          ---   ---
 requests.storage  0     5000Mi


 Name:                                                                            testns-
storagequota
 Resource                                                                         Used  Hard
 --------                                                                         ---   ---
 namespace-service-storage-profile.storageclass.storage.k8s.io/requests.storage  0
9223372036854775807
```

3 Actualice las anotaciones mediante el comando `kubectl annotate`.

   Por ejemplo, `kubectl annotate --overwrite ns testns my-ann="test-ann-3"`

   Para eliminar una anotación, ejecute el comando `kubectl annotate --overwrite ns testns my-ann-`

4 Actualice las etiquetas mediante el comando `kubectl label`.

   Por ejemplo, `kubectl label --overwrite ns testns my-label="test-label-3"`

   Para eliminar una etiqueta, ejecute el comando `kubectl label --overwrite ns testns my-label-`

5 Describa el espacio de nombres para ver las actualizaciones.

```
root@localhost [ /tmp ]# kubectl describe ns testns
Name:         testns
Labels:       my-label=test-label-3
              vSphereClusterID=domain-c50
Annotations:  my-ann: test-ann-3
              vmware-system-namespace-owner-count: 2
              vmware-system-resource-pool: resgroup-153
              vmware-system-resource-pool-cpu-limit: 0.4770
              vmware-system-resource-pool-memory-limit: 2000Mi
              vmware-system-self-service-namespace: true
              vmware-system-vm-folder: group-v154
Status:       Active


Resource Quotas
 Name:             testns
 Resource          Used  Hard
 --------          ---   ---
 requests.storage  0     5000Mi


 Name:                                                                            testns-
storagequota
 Resource                                                                         Used  Hard
 --------                                                                         ---   ---
 namespace-service-storage-profile.storageclass.storage.k8s.io/requests.storage  0
```

```
9223372036854775807


No LimitRange resource.
```

Actualizar un espacio de nombres de autoservicio mediante kubectl edit

El ingeniero de desarrollo y operaciones puede actualizar los espacios de nombres de autoservicio mediante el comando `kubectl edit`.

Requisitos previos

Compruebe que tiene permisos de propietario en el espacio de nombres que desea actualizar.

Procedimiento

1 Inicie sesión en el Clúster Supervisor.

   `kubectl vsphere login --server IP-ADDRESS-SUPERVISOR-CLUSTER --vsphere-username VCENTER-SSO-USERNAME`

2 Describa el espacio de nombres que desea actualizar.

```
kubectl describe ns testns-1
Name:         testns
Labels:       vSphereClusterID=domain-c50
Annotations:  my-ann: test-ann-2
              vmware-system-namespace-owner-count: 2
              vmware-system-resource-pool: resgroup-153
              vmware-system-resource-pool-cpu-limit: 0.4770
              vmware-system-resource-pool-memory-limit: 2000Mi
              vmware-system-self-service-namespace: true
              vmware-system-vm-folder: group-v154
Status:       Active


Resource Quotas
 Name:             testns-1
 Resource          Used  Hard
 --------          ---   ---
 requests.storage  0     5000Mi


 Name:                                                                          testns-1-
storagequota
 Resource                                                                       Used  Hard
 --------                                                                       ---   ---
 namespace-service-storage-profile.storageclass.storage.k8s.io/requests.storage  0
9223372036854775807
```

3 Edite el espacio de nombres mediante el comando `kubectl edit`.

   Por ejemplo, `kubectl edit ns testns-1`

El comando `kubectl edit` abre el manifiesto del espacio de nombres en el editor de texto definido por las variables de entorno KUBE_EDITOR o EDITOR.

4 Actualice las etiquetas.

Por ejemplo, `my-label=test-label`

5 Actualice las anotaciones.

Por ejemplo, `my-ann: test-ann`

6 Describa el espacio de nombres para ver las actualizaciones.

```
root@localhost [ /tmp ]# kubectl describe ns testns-1
Name:         testns-1
Labels:       my-label=test-label
              vSphereClusterID=domain-c50
Annotations:  my-ann: test-ann
              vmware-system-namespace-owner-count: 1
              vmware-system-resource-pool: resgroup-173
              vmware-system-resource-pool-cpu-limit: 0.4770
              vmware-system-resource-pool-memory-limit: 2000Mi
              vmware-system-self-service-namespace: true
              vmware-system-vm-folder: group-v174
Status:       Active


Resource Quotas
 Name:             testns-1
 Resource          Used  Hard
 --------          ---   ---
 requests.storage  0     5000Mi


 Name:                                                                       testns-1-
storagequota
 Resource                                                                    Used  Hard
 --------                                                                    ---   ---
 namespace-service-storage-profile.storageclass.storage.k8s.io/requests.storage  0
9223372036854775807


No LimitRange resource.
```

Eliminar un espacio de nombres de autoservicio

Como ingeniero de desarrollo y operaciones, puede eliminar un espacio de nombres de autoservicio que haya creado.

Requisitos previos

Compruebe si creó un espacio de nombres de autoservicio mediante el complemento de vSphere para kubectl.

Procedimiento

1 Utilice complemento de vSphere para kubectl para autenticarse en clúster supervisor.
Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

2 Elimine el espacio de nombres de autoservicio del clúster.

```
kubectl delete namespace NAMESPACE NAME
```

Por ejemplo:

```
kubectl delete namespace test-ns
```

Administrar servicios de supervisor con vSphere with Tanzu

8

servicios de supervisor son operadores de Kubernetes certificados por vSphere que ofrecen a los desarrolladores componentes de infraestructura como servicio y servicios de proveedores de software independientes perfectamente integrados. Puede instalar y administrar servicios de supervisor en el entorno de vSphere with Tanzu para que estén disponibles para su uso con cargas de trabajo de Kubernetes. Cuando se instalan servicios de supervisor en clústeres supervisor, los ingenieros de desarrollo y operaciones pueden utilizar las API de servicio para crear clústeres supervisor en sus espacios de nombres de usuario. A continuación, estas instancias se pueden consumir en pods de vSphere y clústeres de Tanzu Kubernetes.

Obtenga más información sobre los servicios de supervisor compatibles y cómo descargar sus archivos YAML de servicio en http://vmware.com/go/supervisor-service.

Los servicios de supervisor se administran en la plataforma de servicios de vSphere desde vSphere Client. Mediante el uso de la plataforma, puede administrar el ciclo de vida de servicios de supervisor, instalarlos en clústeres supervisor y realizar el control de versiones. Un servicio de supervisor puede tener varias versiones que puede instalar en clústeres supervisor, ya que solo puede ejecutarse una versión a la vez en una instancia de clúster supervisor.

Tabla 8-1. Estados de servicio de supervisor

Estado	Versión del servicio	Servicio completo
Activo	La versión del servicio está lista para instalarse en la versión de instancias de clústeres supervisor.	Al menos una versión del servicio está en estado activo.
Desactivado	La versión del servicio no se puede instalar en clústeres supervisor. Puede seguir ejecutándose en clústeres supervisor en los que esté instalado, pero no puede instalar una versión desactivada en nuevos clústeres supervisor.	Cuando toda la instancia de servicio de supervisor está desactivada, todas sus versiones también están desactivadas y no se puede instalar ninguna de ellas en clústeres supervisor ni agregar nuevas versiones de servicio hasta que se reactive el servicio.

Operaciones de administración del ciclo de vida de servicios de supervisor

La administración del ciclo de vida de un servicio de supervisor incluye las siguientes operaciones:

- Agregar un nuevo servicio de supervisor a vCenter Server. Cuando se agrega un nuevo servicio a vCenter Server, el servicio y toda la información sobre él se registran en vCenter Server. El servicio aún no está instalado en ningún clúster supervisor. Después de registrar el servicio en vCenter Server, su estado es Activo, lo que significa que puede instalar ese servicio en clústeres supervisor.
- Agregar una nueva versión de servicio de supervisor a vCenter Server. Una vez que haya agregado una instancia de servicio de supervisor a vCenter Server, puede agregar nuevas versiones de ese servicio. Después de registrar la nueva versión del servicio en vCenter Server pasa al estado Activo y puede instalar la versión en clústeres supervisor.
- Instalar un nuevo servicio de supervisor en clústeres supervisor. Cuando se instala un servicio en un clúster supervisor, el archivo YAML de servicio se aplica al clúster, y se crean todos los pods y los recursos necesarios para que funcione el servicio. Cada servicio que se instala en un clúster supervisor tiene un espacio de nombres dedicado en el que se pueden administrar los recursos del servicio. servicios de supervisor también puede tener un complemento de interfaz de usuario para vCenter Server, donde se puede administrar la configuración del servicio.
- Actualizar un servicio de supervisor. Para actualizar un servicio instalado en un clúster supervisor, primero agregue una nueva versión de servicio a vCenter Server y, a continuación, instale la nueva versión en el clúster supervisor. Durante la actualización del servicio, el archivo YAML de la nueva versión se aplica al clúster supervisor. Se eliminarán todos los recursos especificados en la versión anterior del servicio que no sean necesarios para la nueva versión. Por ejemplo, si la versión 1 especifica el pod A y la versión 2 especifica el pod B, después de la actualización a la versión 2, se crea un nuevo pod B y se elimina el pod A. Ninguna carga de trabajo en ejecución actualmente se ve afectada durante el proceso.
- Desinstalar una versión de servicio de supervisor. La desinstalación de una versión de servicio de un clúster supervisor hace que todos los recursos de servicios se eliminen del clúster, incluido el espacio de nombres de servicio. Las instancias de aplicación del servicio en las cargas de trabajo de Kubernetes seguirán ejecutándose.
- Eliminar una versión de servicio de supervisor. Para eliminar una versión del servicio, primero debe desactivar esa versión y desinstalarla de los clústeres supervisor donde se ejecuta. A continuación, puede eliminar la versión del servicio de vCenter Server.
- Eliminar un servicio de supervisor completo. Para eliminar un servicio completo, debe desactivar todas sus versiones, desinstalar estas versiones de clústeres supervisor y, por último, eliminar todas las versiones del servicio.

Este capítulo incluye los siguientes temas:

- Agregar una instancia de servicio de supervisor a vCenter Server
- Instalar un servicio de supervisor en clústeres supervisor

- Acceder a la interfaz de administración de un servicio de supervisor en el clúster supervisor
- Agregar una nueva versión a un servicio de supervisor
- Ver servicios de supervisor instalados en un clúster supervisor
- Desactivar un servicio de supervisor o una versión
- Activar una versión de servicio de supervisor en vCenter Server
- Desinstalar servicio de supervisor de clúster supervisor
- Eliminar una versión del servicio de supervisor
- Eliminar un servicio de supervisor

Agregar una instancia de servicio de supervisor a vCenter Server

Puede agregar servicios de supervisor al sistema vCenter Server donde se ejecuta el entorno de vSphere with Tanzu. Después de agregar servicios a vCenter Server, instale servicios de supervisor en clústeres supervisor para que los ingenieros de desarrollo y operaciones puedan utilizar los servicios en las cargas de trabajo de Kubernetes.

- Obtenga más información sobre los servicios de supervisor compatibles y cómo descargar sus archivos YAML de servicio en http://vmware.com/go/supervisor-service.

Requisitos previos

- Compruebe que tiene el privilegio **Administrar servicios de supervisor** en el sistema vCenter Server donde agrega el servicio.

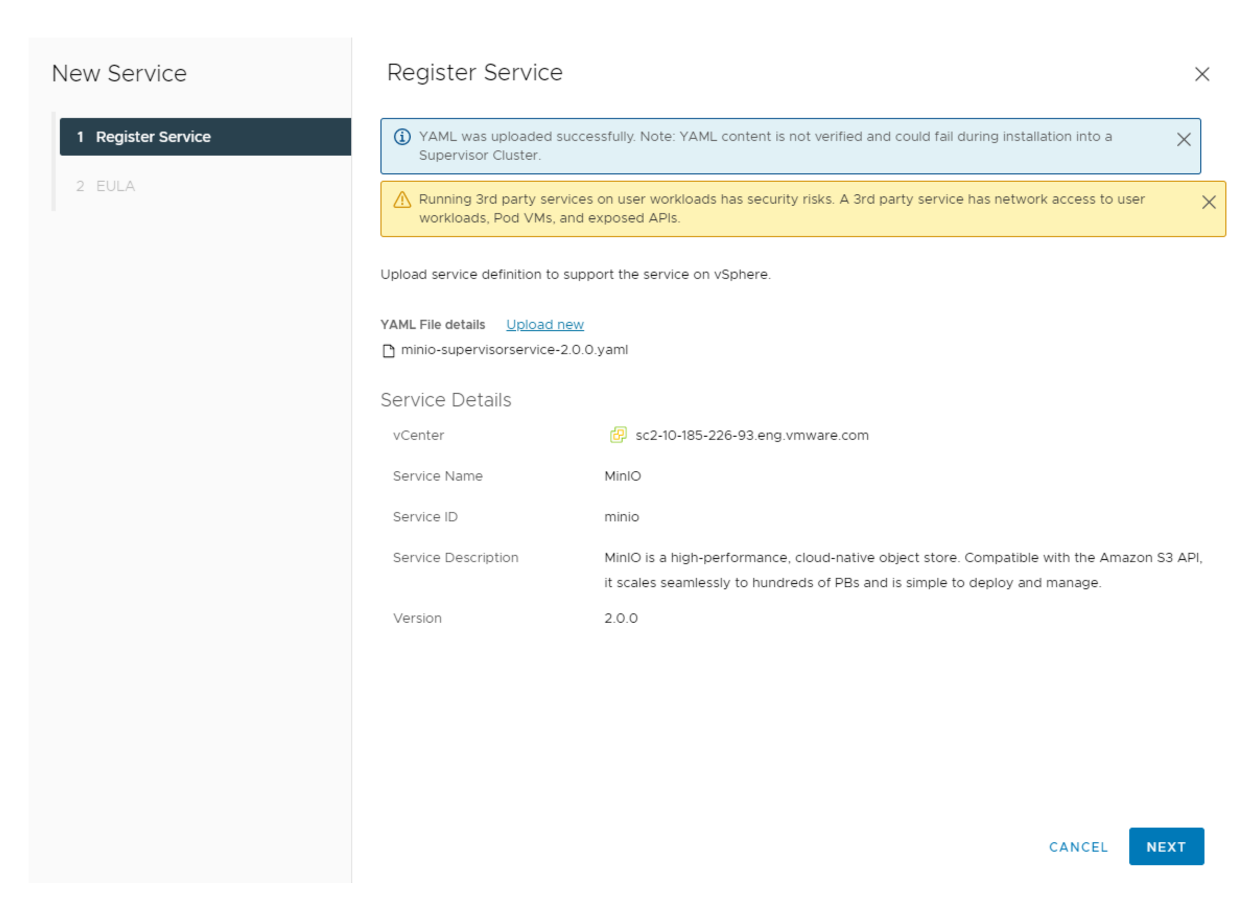
Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione **Servicios**

3 Seleccione un sistema vCenter Server en el menú desplegable de la parte superior.

4 Arrastre y suelte el archivo YAML del servicio en la tarjeta **Agregar nuevo servicio**.

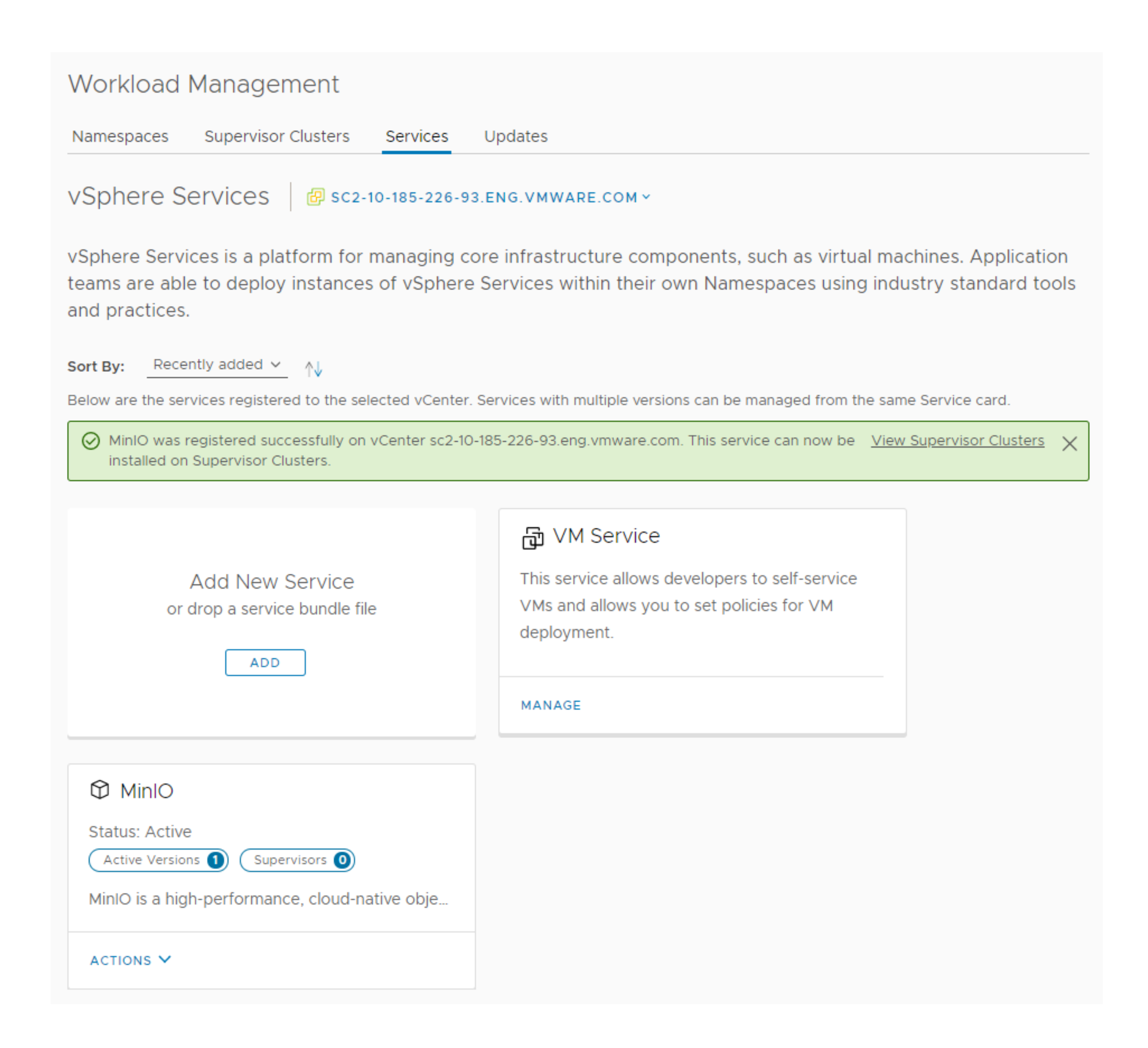


5 Haga clic en **Siguiente** y acepte el CLUF, si existe alguno.

6 Haga clic en **Finalizar**.

Resultados

La instancia de servicio de supervisor y toda su información se registran con el sistema vCenter Server. El servicio está en estado Activo.



Pasos siguientes

Instale la instancia de servicio de supervisor en clústeres supervisor para que los ingenieros de desarrollo y operaciones puedan utilizarlo en las cargas de trabajo de Kubernetes. Consulte Instalar un servicio de supervisor en clústeres supervisor.

Instalar un servicio de supervisor en clústeres supervisor

Tras agregar un servicio de supervisor en vCenter Server, puede instalarlo en los clústeres supervisor del entorno de vSphere with Tanzu. Si instala una versión más reciente de un servicio de supervisor, este reemplazará cualquier versión de servicio anterior que haya en ese clúster supervisor. Solo se puede ejecutar una versión de los clústeres supervisor en un clúster supervisor a la vez.

- Obtenga más información sobre los servicios de supervisor compatibles y cómo descargar sus archivos YAML de servicio en http://vmware.com/go/supervisor-service.

Requisitos previos

- Agregue un nuevo servicio de supervisor o un servicio existente o de una versión más reciente a vCenter Server. Consulte Agregar una instancia de servicio de supervisor a vCenter Server o Agregar una nueva versión a un servicio de supervisor.
- Compruebe que tiene el privilegio **Administrar servicios de supervisor** en el sistema vCenter Server que aloja el clúster supervisor en el que instale el servicio.
- Si el servicio de supervisor requiere de almacenamiento persistente, configure la plataforma de persistencia de datos de vSAN. Consulte Usar la plataforma para la persistencia de datos de vSAN con servicios con estado modernos.

Procedimiento

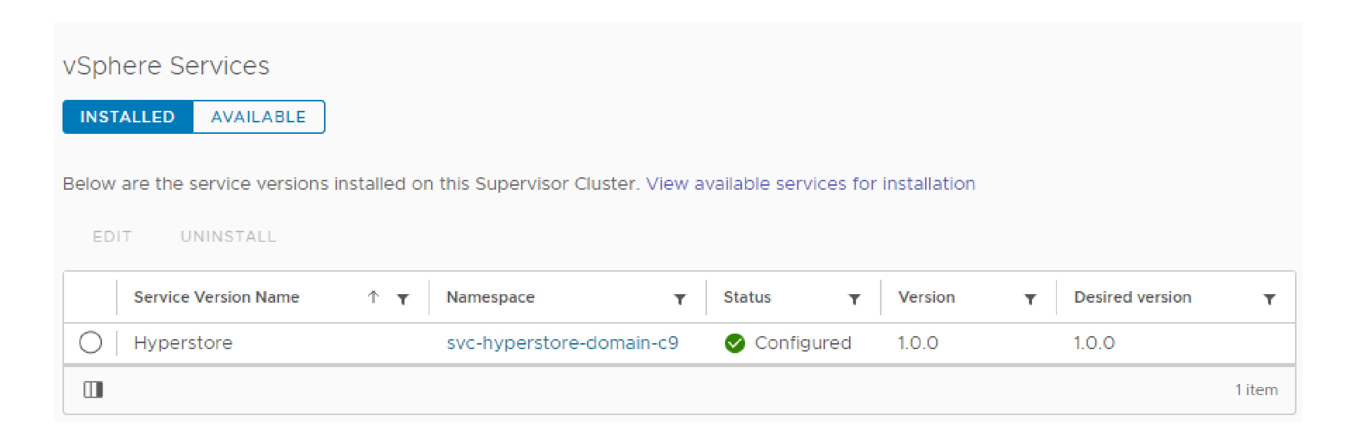
1. En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.
2. Seleccione **Servicios**
3. Seleccione la versión del servicio de supervisor que desea instalar.

   Nota No puede instalar versiones de servicio de supervisor que estén desactivadas.
4. Seleccione el clúster supervisor donde desea instalar el servicio.
5. Rellene el endpoint del registro, el nombre de usuario y la contraseña si ha alojado las imágenes en un registro privado.

   Es posible que existan otros pares de clave-valor en caso de que el servicio los requiera. Consulte la documentación del servicio para obtener más información.

Resultados

El estado del servicio de supervisor es Configurando, lo que significa que todos los recursos necesarios se crean en el clúster supervisor y el YAML de servicio se aplica al clúster. Una vez que el YAML se aplique correctamente en el clúster supervisor con todos sus recursos y el espacio de nombres creados o actualizados, el estado del servicio pasará a ser Configurado. El servicio está disponible para todos los espacios de nombres de ese clúster, y los ingenieros de desarrollo y operaciones pueden utilizarlo con sus cargas de trabajo de Kubernetes.



Nota El clúster supervisor no supervisa si el servicio de supervisor funciona realmente. Por ejemplo, si especificó un nombre de usuario o una contraseña del registro incorrectos, es posible que el servicio no pueda recuperar ninguna de las imágenes que necesita para ejecutarse. De esta manera, el servicio puede aparecer como Configurado aunque no funcione en realidad. Para confirmar si el servicio de supervisor funciona o no, compruebe el espacio de nombres del servicio y los pods en ejecución.

Pasos siguientes

Configure el servicio de supervisor mediante la interfaz. Consulte dónde se puede encontrar en Acceder a la interfaz de administración de un servicio de supervisor en el clúster supervisor.

Acceder a la interfaz de administración de un servicio de supervisor en el clúster supervisor

Compruebe dónde encontrar la interfaz de usuario de administración de servicios de supervisor una vez que la instale en un clúster supervisor. Los servicios de supervisor pueden proporcionar su propio complemento de interfaz de usuario para vCenter Server que agrega la interfaz de servicio a la vista del clúster supervisor en vSphere Client. En función de los detalles de servicio de supervisor, puede utilizar su interfaz para configurar y administrar el servicio también para implementar instancias de servicio de ese servicio.

Procedimiento

1 En vSphere Client, desplácese hasta clúster supervisor.

2 Seleccione **Configurar** y desplácese hacia abajo hasta la interfaz de servicio, a la que se le suele poner el nombre del servicio, por ejemplo, **MinIO**.

Agregar una nueva versión a un servicio de supervisor

Una vez que haya agregado un servicio de supervisor a vCenter Server en el que tiene el entorno de vSphere with Tanzu, puede agregar una nueva versión a ese servicio. Puede instalar diferentes versiones de servicio en clústeres supervisor.

- Obtenga más información sobre los servicios de supervisor compatibles y cómo descargar sus archivos YAML de servicio en http://vmware.com/go/supervisor-service.

Requisitos previos

- Agregue el servicio a vCenter Server. Consulte Agregar una instancia de servicio de supervisor a vCenter Server.
- Compruebe que tiene el privilegio **Administrar servicios de supervisor** en el sistema vCenter Server donde agrega la nueva versión del servicio.

Procedimiento

1. En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.
2. Seleccione **Servicios**
3. En la tarjeta del servicio al que desea agregar una nueva versión, seleccione **Acciones > Agregar nueva versión**.
4. Cargue el archivo YAML de la nueva versión del servicio y haga clic en **Siguiente**.
5. Acepte el CLUF si lo hubiera y haga clic en **Finalizar**.

Resultados

Se agrega la nueva versión del servicio y se encuentra en estado activo.

Pasos siguientes

Instale la nueva versión del servicio en clústeres supervisor. Consulte Instalar un servicio de supervisor en clústeres supervisor.

Ver servicios de supervisor instalados en un clúster supervisor

Vea los servicios de vSphere instalados en los clústeres supervisor del entorno de vSphere with Tanzu. Los servicios de supervisor instalados en un clúster supervisor están disponibles para cada espacio de nombres en el clúster.

Requisitos previos

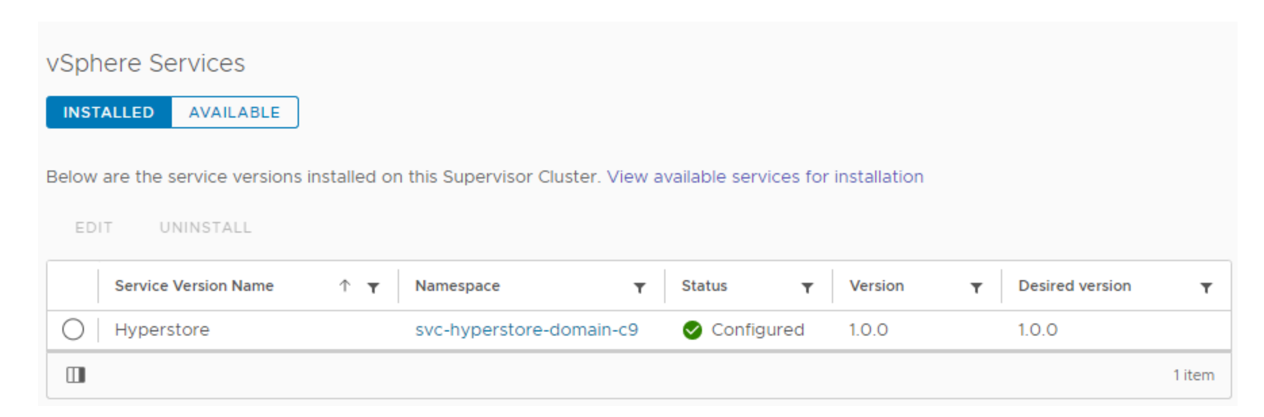
- Agregue servicios de supervisor a vCenter Server. Consulte Agregar una instancia de servicio de supervisor a vCenter Server.
- Instale servicios de supervisor en clústeres supervisor. Consulte Instalar un servicio de supervisor en clústeres supervisor.

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione la pestaña **Clústeres supervisores**.

3 En una instancia de clúster supervisor, en la columna **Servicios**, haga clic en **Ver**.



- En la pestaña **Instalado**, vea los servicios de supervisor que están instalados actualmente en el clúster supervisor.
- En la pestaña **Disponible**, vea los servicios de supervisor disponibles para instalación.

Pasos siguientes

Puede administrar los servicios de supervisor en ese clúster supervisor, desinstalar servicios o instalar otros nuevos desde los servicios en la pestaña **Disponible**.

Desactivar un servicio de supervisor o una versión

Desactive una versión del servicio de supervisor si ya no desea utilizarla con cargas de trabajo de Kubernetes en su entorno de vSphere with Tanzu. Una versión de servicio desactivada sigue ejecutándose en los clústeres supervisor en los que se ha instalado, pero no es posible instalar una versión de servicio desactivada en otros clústeres supervisor. Cuando se desactiva un servicio completo, todas las versiones del servicio se desactivan, por lo que no es posible agregar nuevas versiones de servicio ni instalarlas en los clústeres supervisor hasta que se reactive el servicio.

Requisitos previos

- Compruebe que tiene el privilegio **Administrar servicios de supervisor** en el nivel de vCenter Server.

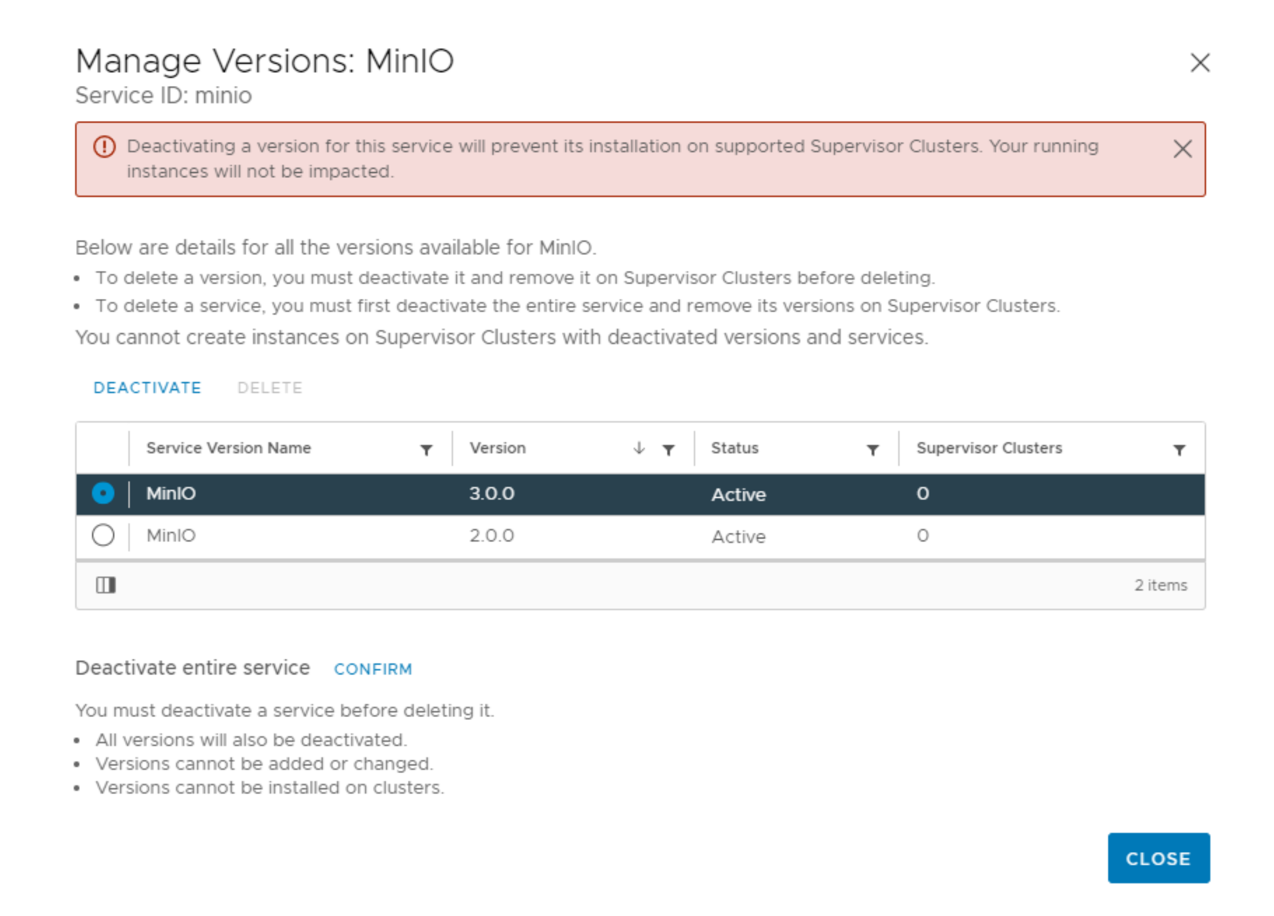
Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione **Servicios**

3 En la tarjeta de servicio, seleccione **Acciones > Administrar versiones**.

- Para desactivar una versión del servicio de supervisor, seleccione la versión y haga clic en **Desactivar**.
- Para desactivar todo el servicio, haga clic en **Confirmar** junto a **Desactivar todo el servicio**.



Resultados

La versión del servicio está desactivada y no es posible instalar en los clústeres supervisor.

Activar una versión de servicio de supervisor en vCenter Server

Una vez que se desactiva una versión de servicio de supervisor, puede volver a activarla en caso de que el equipo de desarrollo y operaciones desee utilizar esa versión de servicio en las cargas de trabajo de Kubernetes que se ejecutan en vSphere with Tanzu.

- Compruebe que tiene el privilegio **Administrar servicios de supervisor** en el sistema vCenter Server en el que está registrado el servicio.

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione **Servicios**

3 En la tarjeta de servicio de supervisor, haga clic en **Versiones activas**.

4 Seleccione **Administrar versiones**.

5 Seleccione la versión de servicio de supervisor en estado Desactivado y haga clic en **Reactivar**.

Desinstalar servicio de supervisor de clúster supervisor

Desinstale servicio de supervisor de clúster supervisor si el equipo de desarrollo y operaciones ya no necesita ese servicio para las cargas de trabajo de Kubernetes que se ejecutan en el entorno de vSphere with Tanzu.

Requisitos previos

- Compruebe que tiene el privilegio **Administrar servicios de supervisor** en el sistema vCenter Server que aloja la instancia de clúster supervisor en la que está instalado el servicio.

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione instancias de **Supervisor Cluster**.

3 En una instancia de clúster supervisor, en la columna **Servicios**, haga clic en **Ver**.

4 Seleccione la instancia de servicio de supervisor que desea desinstalar y haga clic en **Desinstalar**.

Resultados

servicio de supervisor se desinstala de clúster supervisor. Todos los recursos de servicios y el espacio de nombres de servicio se eliminan del clúster supervisor. Todas las instancias administradas de servicios que utilizan la plataforma de persistencia de datos vSAN se eliminan del clúster supervisor.

Eliminar una versión del servicio de supervisor

Elimine la versión de un servicio de supervisor de vCenter Server si esta versión está obsoleta y su equipo de desarrollo y operaciones ya no la necesita para la carga de trabajo de Kubernetes que se ejecuta en el entorno de vSphere with Tanzu.

Requisitos previos

- Compruebe que la versión del servicio de supervisor que desea eliminar no está instalada en clústeres supervisor. Consulte Desinstalar servicio de supervisor de clúster supervisor.

- Compruebe que tiene el privilegio **Administrar servicios de supervisor** en el nivel de vCenter Server.

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione **Servicios**

3 En la tarjeta del servicio de supervisor, seleccione **Acciones > Administrar versiones**.

4 Seleccione la versión que desee eliminar y haga clic en **Desactivar**.

5 Seleccione la versión desactivada y haga clic en **Eliminar**.

Eliminar un servicio de supervisor

Elimine un servicio de supervisor del entorno de vSphere with Tanzu si sus ingenieros de desarrollo y operaciones ya no lo necesitan para sus cargas de trabajo de Kubernetes.

Requisitos previos

- Compruebe que tiene el privilegio **Administrar servicios de supervisor** en el sistema vCenter Server en el que está registrado el servicio.

Procedimiento

1 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

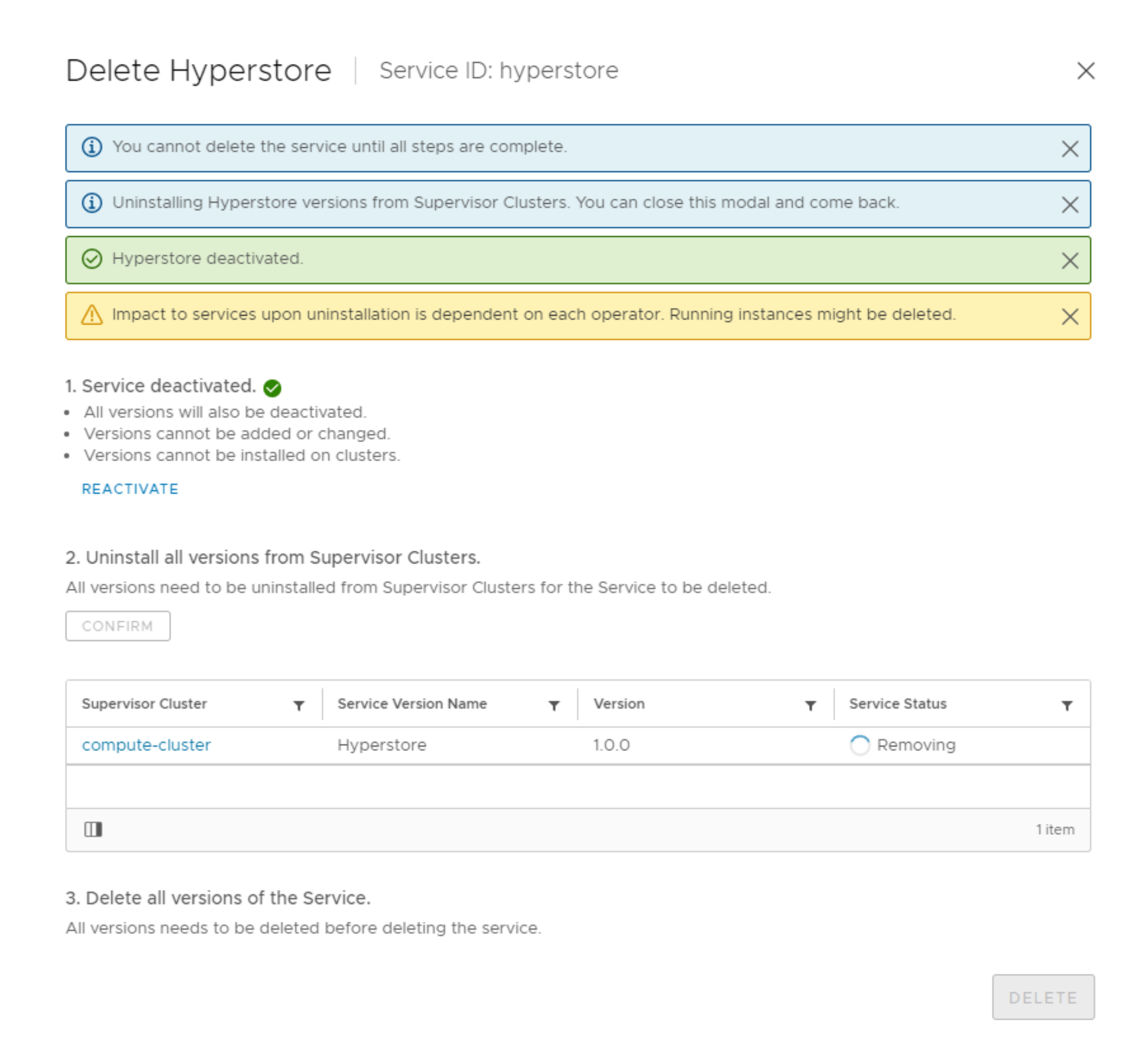
2 Seleccione **Servicios**

3 En la tarjeta del servicio de supervisor que desea eliminar, seleccione **Acciones > Eliminar**.

4 Confirme la desactivación de todas las versiones de servicio disponibles actualmente.

5 Confirme la desinstalación del servicio de los clústeres supervisor.

   La desinstalación de un servicio de supervisor del clústeres supervisor en el que se ejecuta puede tardar algún tiempo. Puede cerrar el cuadro de diálogo mientras se completa el proceso y, a continuación, volver a abrirlo para continuar con la siguiente fase.



6 Confirme la eliminación de todas las versiones disponibles del servicio.

7 Haga clic en **Eliminar**.

Conectarse a clústeres de vSphere with Tanzu

9

Conéctese al clúster supervisor para aprovisionar los clústeres de Tanzu Kubernetes. Una vez aprovisionados, podrá conectarse a los clústeres de Tanzu Kubernetes mediante diversos métodos y autenticarse según su función y su objetivo.

Este capítulo incluye los siguientes temas:

- Descargar e instalar Herramientas de la CLI de Kubernetes para vSphere
- Configurar el inicio de sesión seguro para clústeres de vSphere with Tanzu
- Conectarse al clúster supervisor como usuario vCenter Single Sign-On
- Autenticarse con clústeres de Tanzu Kubernetes
- Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On
- Conectarse al plano de control del clúster de Tanzu Kubernetes como el administrador
- Conectarse mediante SSH a nodos de clúster de Tanzu Kubernetes como usuario del sistema con una clave privada
- Conectarse mediante SSH a nodos de clúster de Tanzu Kubernetes como usuario del sistema con una contraseña
- Conceder acceso de desarrollador a clústeres de Tanzu Kubernetes

Descargar e instalar Herramientas de la CLI de Kubernetes para vSphere

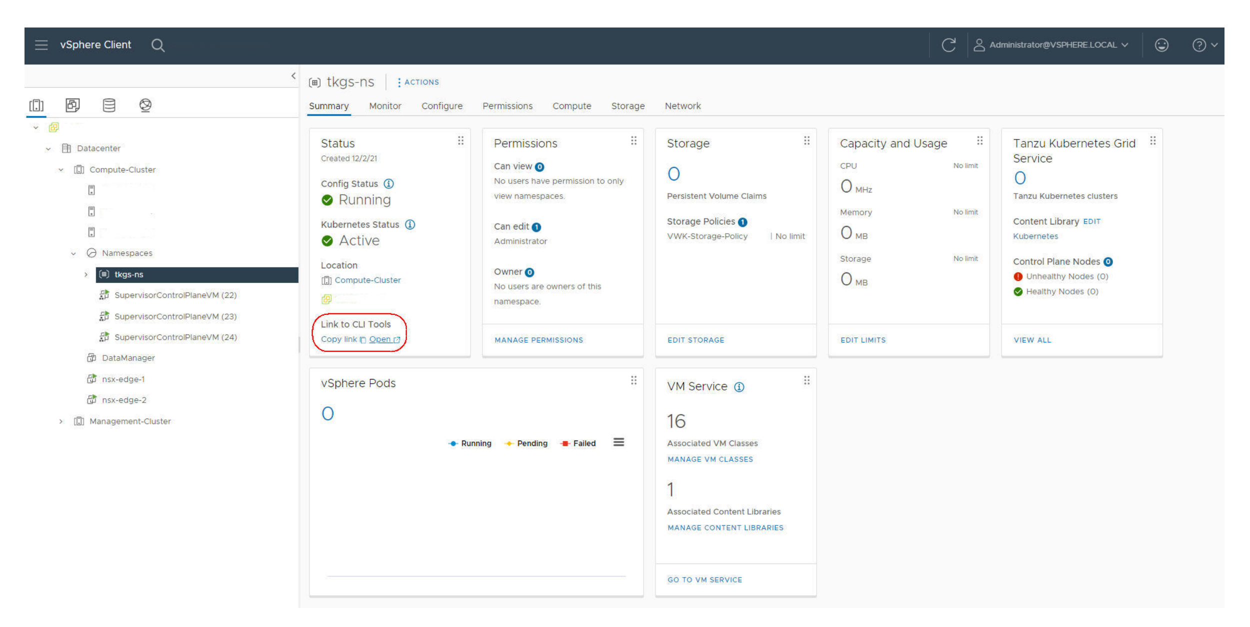
Puede utilizar Herramientas de la CLI de Kubernetes para vSphere para ver y controlar los espacios de nombres y los clústeres de vSphere with Tanzu.

El paquete de descarga de Herramientas de la CLI de Kubernetes incluye dos ejecutables: el kubectl de código abierto estándar y el complemento de vSphere para kubectl. La CLI de kubectl tiene una arquitectura acoplable. El complemento de vSphere para kubectl extiende los comandos disponibles a kubectl de modo que se conecte al clúster supervisor y a clústeres de Tanzu Kubernetes mediante credenciales de vCenter Single Sign-On.

Nota Como práctica recomendada, una vez que haya realizado una actualización del espacio de nombres de vSphere y haya actualizado el clúster supervisor, actualice también el complemento de vSphere para kubectl. Consulte Actualizar complemento de vSphere para kubectl.

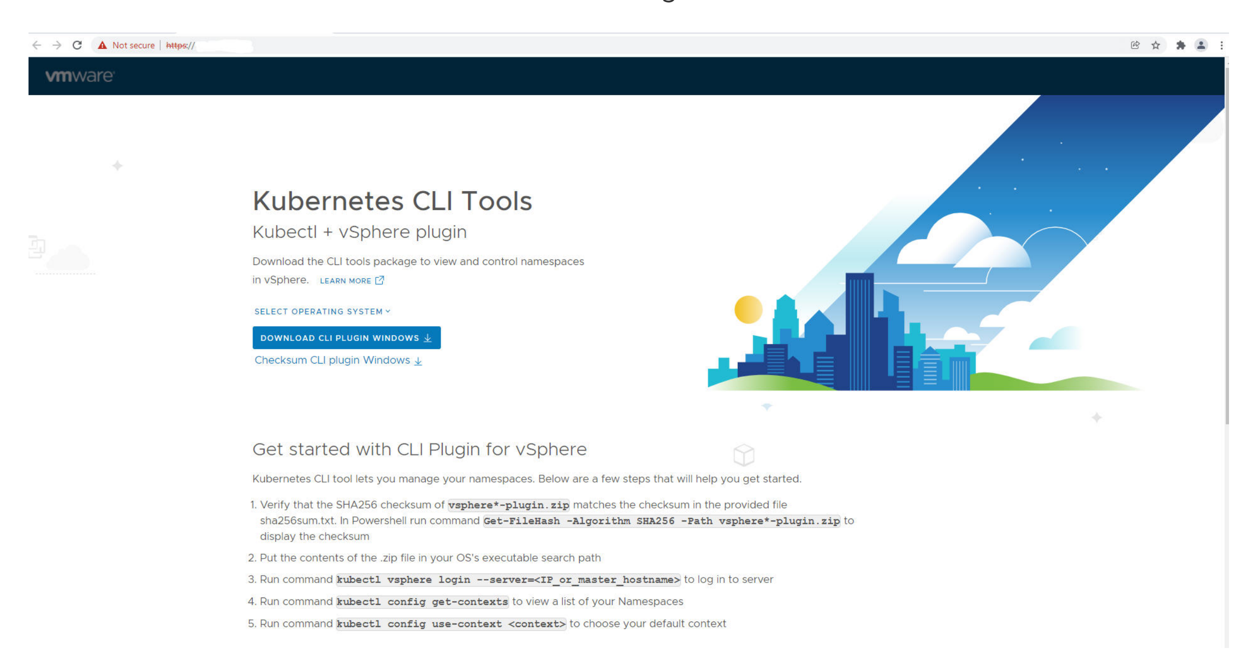
Requisitos previos

- Obtenga de su administrador de vSphere el vínculo de la página de descargas Herramientas de la CLI de Kubernetes.
- De forma alternativa, si tiene acceso a la instancia de vCenter Server, obtenga el vínculo de la siguiente manera:
  - Inicie sesión en vCenter Server mediante vSphere Client.
  - Desplácese hasta **vSphere clúster > Espacios de nombres** y seleccione el espacio de nombres de vSphere en el que está trabajando. En el ejemplo que se muestra a continuación, este es el espacio de nombres "tkgs-ns" que creamos para nuestros clústeres de Tanzu Kubernetes.
  - Seleccione la pestaña **Resumen** y encuentre el área **Estado** en esta página.
  - Seleccione **Abrir** debajo del encabezado **Vínculo a herramientas de CLI** para abrir la página de descargas. O bien, puede **Copiar** el vínculo.



Procedimiento

1 Con un navegador, vaya a la URL de descarga de **Herramientas de la CLI de Kubernetes** correspondiente a su entorno. Consulte la sección de requisitos previos anterior para obtener instrucciones sobre cómo ubicar la URL de descarga.



2 Seleccione el sistema operativo.

3 Descargue el archivo `vsphere-plugin.zip`.

4 Extraiga el contenido del archivo ZIP en un directorio de trabajo.

El paquete `vsphere-plugin.zip` contiene dos archivos ejecutables: kubectl y complemento de vSphere para kubectl. `kubectl` es la CLI de Kubernetes estándar. `kubectl-vsphere` es el complemento de vSphere para kubectl que lo ayudará a autenticarse en el clúster supervisor y en los clústeres de Tanzu Kubernetes utilizando sus credenciales de vCenter Single Sign-On.

5 Agregue la ubicación de los dos archivos ejecutables a la variable PATH del sistema.

6 Para comprobar la instalación de la CLI de kubectl, inicie una sesión de Shell, de terminal o de línea de comandos y ejecute el comando `kubectl`.

Verá el mensaje de aviso de kubectl y la lista de opciones de línea de comandos para la CLI.

7 Para comprobar la instalación de complemento de vSphere para kubectl, ejecute el comando `kubectl vsphere`.

Verá el mensaje de aviso de complemento de vSphere para kubectl y la lista de opciones de línea de comandos para el complemento.

Pasos siguientes

Configurar el inicio de sesión seguro para clústeres de vSphere with Tanzu.

Configurar el inicio de sesión seguro para clústeres de vSphere with Tanzu

Para iniciar sesión de forma segura en clústeres de vSphere with Tanzu, incluidos los clústeres de clúster supervisor y Tanzu Kubernetes, configure el complemento complemento de vSphere para kubectl con el certificado TLS adecuado y asegúrese de que esté ejecutando la edición más reciente del complemento.

Certificado de CA de clúster supervisor

vSphere with Tanzu admite vCenter Single Sign-On para el acceso a los clústeres mediante el comando de complemento de vSphere para kubectl `kubectl vsphere login …`. Para instalar y utilizar esta utilidad, consulte Descargar e instalar Herramientas de la CLI de Kubernetes para vSphere.

El complemento complemento de vSphere para kubectl establece de forma predeterminada el inicio de sesión seguro y requiere un certificado de confianza, el certificado firmado por la entidad de certificación raíz vCenter Server. A pesar de que el complemento es compatible con la marca de `--insecure-skip-tls-verify`, por motivos de seguridad, esto no se recomienda.

Para iniciar sesión de forma segura en los clústeres de clúster supervisor y Tanzu Kubernetes mediante el complemento complemento de vSphere para kubectl, tiene dos opciones:

Opción	Instrucciones
Descargue e instale el certificado de la entidad de certificación de vCenter Server raíz en cada máquina cliente.	Consulte el artículo VMware de la base de conocimientos Cómo descargar e instalar certificados raíz de vCenter Server.
Reemplace el certificado VIP utilizado para clúster supervisor por un certificado firmado por una entidad de certificación de confianza de cada máquina cliente.	Consulte Reemplazar el certificado VIP para conectarse de forma segura al endpoint de API de clúster supervisor.

Nota Para obtener información adicional sobre la autenticación de vSphere, incluidos vCenter Single Sign-On, la administración y rotación de certificados de vCenter Server y la solución de problemas de autenticación, consulte la documentación de autenticación de vSphere.

Certificado de CA del clúster de Tanzu Kubernetes

Para conectarse de forma segura con el servidor de API del clúster de Tanzu Kubernetes mediante la CLI `kubectl`, debe descargar el certificado de CA del clúster de Tanzu Kubernetes.

Si utiliza la edición más reciente de complemento de vSphere para kubectl, la primera vez que inicie sesión en el clúster de Tanzu Kubernetes, el complemento registra el certificado de la entidad de certificación del clúster de Tanzu Kubernetes en el archivo kubconfig. Este certificado se almacena en el secreto de Kubernetes denominado *`TANZU-KUBERNETES-CLUSTER-NAME`*`-ca`. El complemento utiliza este certificado para rellenar la información de CA en el almacén de datos de la entidad de certificación del clúster correspondiente.

Si va a actualizar vSphere with Tanzu, asegúrese de hacerlo a la versión más reciente del complemento. Consulte Actualizar complemento de vSphere para kubectl.

Conectarse al clúster supervisor como usuario vCenter Single Sign-On

Para aprovisionar los pods de vSphere o los clústeres de Tanzu Kubernetes mediante servicio Tanzu Kubernetes Grid, conéctese al clúster supervisor mediante el complemento de vSphere para kubectl y autentíquese con las credenciales de vCenter Single Sign-On.

Después de iniciar sesión en clúster supervisor, el complemento de vSphere para kubectl genera el contexto del clúster. En Kubernetes, un contexto de configuración incluye un clúster, un espacio de nombres y un usuario. Puede ver el contexto del clúster en el archivo `.kube/config`. Generalmente, este archivo se denomina `kubeconfig`.

Nota Si ya tiene un archivo `kubeconfig`, este se anexa a cada contexto de clúster. El complemento de vSphere para kubectl respeta la variable de entorno KUBECONFIG que kubectl utiliza. Aunque no es obligatorio, puede que resulte útil definir esta variable antes de ejecutar `kubectl vsphere login ...` para que la información se escriba en un archivo nuevo (en lugar de agregarse al archivo `kubeconfig` actual).

Requisitos previos

- Obtenga las credenciales de vCenter Single Sign-On.
- Obtenga la dirección IP del plano de control de clúster supervisor.
- Obtenga el nombre de la instancia de espacio de nombres de vSphere.
- Obtenga la confirmación de que tiene permisos **Editar** en espacio de nombres de vSphere.
- Descargar e instalar Herramientas de la CLI de Kubernetes para vSphere.
- Para comprobar que el certificado ofrecido por el plano de control de Kubernetes sea de confianza en el sistema, instale la CA de firma como raíz de confianza o agregue el certificado directamente como raíz de confianza. Consulte Configurar el inicio de sesión seguro para clústeres de vSphere with Tanzu.

Procedimiento

1 Para ver la sintaxis y las opciones de los comandos para iniciar sesión, ejecute el siguiente comando.

```
kubectl vsphere login --help
```

2 Para conectarse a clúster supervisor, ejecute el siguiente comando.

```
kubectl vsphere login --server=<KUBERNETES-CONTROL-PLANE-IP-ADDRESS> --vsphere-username
<VCENTER-SSO-USER>
```

Por ejemplo:

```
kubectl vsphere login --server=10.92.42.13 --vsphere-username administrator@example.com
```

Esta acción crea un archivo de configuración con el token web de JSON (JSON Web Token, JWT) para autenticarse en la API de Kubernetes.

3 Para autenticarse, introduzca la contraseña del usuario.

   Después de conectarse a clúster supervisor, se le mostrarán los contextos de configuración a los que puede acceder. Por ejemplo:

```
You have access to the following contexts:
tanzu-ns-1
tkg-cluster-1
tkg-cluster-2
```

4 Para ver los detalles de los contextos de configuración a los que puede acceder, ejecute el siguiente comando de `kubectl`:

```
kubectl config get-contexts
```

   La CLI muestra los detalles de cada contexto disponible.

5 Para cambiar de contexto, utilice el siguiente comando:

```
kubectl config use-context <example-context-name>
```

Pasos siguientes

Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.

Autenticarse con clústeres de Tanzu Kubernetes

De acuerdo con su función y su propósito, puede autenticarse con el entorno de clústeres de Tanzu Kubernetes de varias maneras.

Los ingenieros de desarrollo y operaciones aprovisionan y operan clústeres de Tanzu Kubernetes. Los desarrolladores implementan cargas de trabajo en clústeres de Tanzu Kubernetes. Es posible que los administradores deban solucionar problemas en los clústeres de Tanzu Kubernetes. vSphere with Tanzu proporciona métodos de autenticación que respaldan cada función u objetivo.

- Los ingenieros de desarrollo y operaciones se conectan a clúster supervisor para aprovisionar y actualizar clústeres de Tanzu Kubernetes. La autenticación se realiza mediante el complemento de vSphere para kubectl y las credenciales de vCenter Single Sign-On. Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

- Los administradores de clústeres se conectan a un clúster de Tanzu Kubernetes aprovisionado para operarlo y administrarlo.
  - A un usuario con el permiso **Editar** en la instancia de espacio de nombres de vSphere en la que se implementó el clúster se le asigna la función `cluster-admin`. Los administradores de clústeres se autentican con el complemento de vSphere para kubectl y sus credenciales de vCenter Single Sign-On. Consulte Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.
  - Opcionalmente, los administradores de clústeres pueden conectarse a un clúster de Tanzu Kubernetes como el usuario `kubernetes-admin`. Este método puede resultar apropiado si la autenticación de vCenter Single Sign-On no está disponible. Consulte Conectarse al plano de control del clúster de Tanzu Kubernetes como el administrador.
- Los usuarios o los desarrolladores de clústeres se conectan a un clúster de Tanzu Kubernetes para implementar cargas de trabajo, incluidos pods, servicios, equilibradores de carga y otros recursos.
  - Un administrador de clústeres concede a los desarrolladores acceso al clúster enlazando el usuario o el grupo a la directiva de seguridad de pods predeterminada o personalizada. Para obtener más información, consulte Conceder acceso de desarrollador a clústeres de Tanzu Kubernetes.
  - Los desarrolladores enlazados se autentican con clústeres de Tanzu Kubernetes mediante el complemento de vSphere para kubectl y sus credenciales de vCenter Single Sign-On. Consulte Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.
- Con el fin de solucionar problemas, los administradores de sistemas pueden conectarse a un clúster de Tanzu Kubernetes como `vmware-system-user` mediante SSH y una clave privada. Consulte Conectarse mediante SSH a nodos de clúster de Tanzu Kubernetes como usuario del sistema con una clave privada.

Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On

Puede conectarse a un clúster de Tanzu Kubernetes mediante el complemento de vSphere para kubectl y autenticarse con las credenciales de vCenter Single Sign-On.

Después de iniciar sesión en el clúster de Tanzu Kubernetes, el complemento de vSphere para kubectl genera el contexto del clúster. En Kubernetes, un contexto de configuración incluye un clúster, un espacio de nombres y un usuario. Puede ver el contexto del clúster en el archivo `.kube/config`. Generalmente, este archivo se denomina `kubeconfig`.

Nota Si ya tiene un archivo `kubeconfig`, este se anexa a cada contexto de clúster. El complemento de vSphere para kubectl respeta la variable de entorno KUBECONFIG que kubectl utiliza. Aunque no es obligatorio, puede que resulte útil definir esta variable antes de ejecutar `kubectl vsphere login ...` para que la información se escriba en un archivo nuevo (en lugar de agregarse al archivo `kubeconfig` actual).

Requisitos previos

Obtenga la siguiente información del administrador de vSphere:

- Obtenga las credenciales de vCenter Single Sign-On.
- Obtenga la dirección IP del plano de control de clúster supervisor.
- Obtenga el nombre de la instancia de espacio de nombres de vSphere.
- Descargar e instalar Herramientas de la CLI de Kubernetes para vSphere.

Procedimiento

1 Para ver la sintaxis y las opciones de los comandos para iniciar sesión, ejecute el siguiente comando.

```
kubectl vsphere login --help
```

2 Para conectarse al clúster de Tanzu Kubernetes, ejecute el siguiente comando.

```
kubectl vsphere login --server=SUPERVISOR-CLUSTER-CONTROL-PLANE-IP
--tanzu-kubernetes-cluster-name TANZU-KUBERNETES-CLUSTER-NAME
--tanzu-kubernetes-cluster-namespace SUPERVISOR-NAMESPACE-WHERE-THE-CLUSTER-IS-DEPLOYED
--vsphere-username VCENTER-SSO-USER-NAME
```

Por ejemplo:

```
kubectl vsphere login --server=10.92.42.137
--tanzu-kubernetes-cluster-name tanzu-kubernetes-cluster-01
--tanzu-kubernetes-cluster-namespace tanzu-ns-1
--vsphere-username administrator@example.com
```

Esta acción crea un archivo de configuración con el token web de JSON (JSON Web Token, JWT) para autenticarse en la API de Kubernetes.

3 Para autenticarse, introduzca la contraseña de vCenter Single Sign-On.

Si la operación se realiza correctamente, aparecerá el mensaje `Logged in successfully` y podrá ejecutar comandos de kubectl en el clúster. Si el comando devuelve el error `Error from server (Forbidden)`, es posible que no tenga los permisos necesarios. Para obtener más información, consulte Solucionar errores de conexión de vCenter Single Sign-On.

4 Para obtener una lista de los contextos a su disposición, ejecute el siguiente comando:

```
kubectl config get-contexts
```

Este comando muestra los contextos de configuración a los que puede acceder. Debe ver un contexto de configuración para el clúster de destino como, por ejemplo, `tkg-cluster-01`.

5 Para usar el contexto del clúster de destino, ejecute el siguiente comando:

```
kubectl config use-context CLUSTER-NAME
```

6 Para enumerar los nodos de clúster, ejecute el siguiente comando:

```
kubectl get nodes
```

Verá el plano de control y los nodos de trabajo de este clúster.

7 Para enumerar todos los pods de clúster, ejecute el siguiente comando:

```
kubectl get pods -A
```

Verá todos los pods de este clúster en todos los espacios de nombres de Kubernetes a los que puede acceder. Si no implementó ninguna carga de trabajo, no verá ningún pod en el espacio de nombres predeterminado.

Conectarse al plano de control del clúster de Tanzu Kubernetes como el administrador

Puede conectarse al plano de control del clúster de Tanzu Kubernetes como el usuario `kubernetes-admin` para realizar tareas administrativas y solucionar problemas del clúster.

Un archivo `kubeconfig` válido para un clúster de Tanzu Kubernetes aprovisionado está disponible en clúster supervisor como un objeto secreto denominado *`TKGS-CLUSTER-NAME`*`-kubeconfig`. Puede utilizar este secreto para conectarse al plano de control del clúster como el usuario `kubernetes-admin`. Para obtener más información, consulte Obtener los secretos del clúster de Tanzu Kubernetes.

Procedimiento

1 Conéctese al clúster supervisor. Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

2 Cambie el contexto al espacio de nombres de vSphere donde se aprovisiona el clúster de Tanzu Kubernetes de destino.

```
kubectl config use-context VSPHERE-NAMESPACE
```

3 Vea los objetos secretos en el espacio de nombres.

```
kubectl get secrets
```

El secreto se denomina *TKGS-CLUSTER-NAME*-kubeconfig.

```
kubectl config use-context tkgs-cluster-ns
Switched to context "tkgs-cluster-ns".
ubuntu@ubuntu:~$ kubectl get secrets
NAME                                   TYPE                                  DATA   AGE
...
tkgs-cluster-1-kubeconfig              Opaque                                1      23h
...
```

4 Ejecute el siguiente comando para descodificar el secreto.

El secreto está codificado en Base64. Para descodificarlo: en Linux, utilice `base64 --decode` (o `base64 -d`); en MacOS, utilice `base64 --Decode` (o `base64 -D`); en Windows, utilice una herramienta en línea.

```
kubectl get secret TKGS-CLUSTER-NAME-kubeconfig -o jsonpath='{.data.value}' | base64 -d >
tkgs-cluster-kubeconfig-admin
```

Este comando descodifica el secreto y lo escribe en un archivo local denominado `tkgs-cluster-kubeconfig-admin`. Utilice el comando `cat` para comprobar el contenido del archivo.

5 Conéctese al clúster de Tanzu Kubernetes como el administrador de Kubernetes usando el archivo `tkgs-cluster-kubeconfig-admin` decodificado.

Existen dos opciones para realizar esta acción:

Opción	Descripción
--kubeconfig <path\to\kubeconfig>	Utilice la marca `--kubeconfig` y la ruta de acceso al archivo kubeconfig local. Por ejemplo, si suponemos que el archivo kubeconfig se encuentra en el mismo directorio en el que se ejecuta el comando: `kubectl --kubeconfig tkgs-cluster-kubeconfig-admin get nodes`
KUBECONFIG	Establezca la variable de entorno KUBECONFIG para que apunte al archivo kubeconfig descodificado y ejecute kubectl, como `kubectl get nodes`.

Debería ver los nodos en el clúster. Por ejemplo:

```
kubectl --kubeconfig tkgs-cluster-kubeconfig-admin get nodes
NAME                                          STATUS   ROLES    AGE   VERSION
tkgs-cluster-1-control-plane-4ncm4            Ready    master   23h   v1.18.5+vmware.1
tkgs-cluster-1-control-plane-jj9gq            Ready    master   23h   v1.18.5+vmware.1
```

```
tkgs-cluster-1-control-plane-r4hm6              Ready    master   23h   v1.18.5+vmware.1
tkgs-cluster-1-workers-6njk7-84dd7f48c6-nz2n8   Ready    <none>   23h   v1.18.5+vmware.1
tkgs-cluster-1-workers-6njk7-84dd7f48c6-rk9pk   Ready    <none>   23h   v1.18.5+vmware.1
tkgs-cluster-1-workers-6njk7-84dd7f48c6-zzngh   Ready    <none>   23h   v1.18.5+vmware.1
```

Conectarse mediante SSH a nodos de clúster de Tanzu Kubernetes como usuario del sistema con una clave privada

Puede conectarse mediante SSH a un nodo de clúster de Tanzu Kubernetes como `vmware-system-user` con una clave privada.

Puede conectarse mediante SSH a cualquier nodo del clúster de Tanzu Kubernetes como usuario `vmware-system-user`. El secreto que contiene la clave privada SSH se denomina `CLUSTER-NAME-ssh`. Para obtener más información, consulte Obtener los secretos del clúster de Tanzu Kubernetes.

Para conectarse a un nodo del clúster de Tanzu Kubernetes a través de SSH mediante una clave privada, cree un pod de vSphere de Jump Box en el clúster supervisor.

Requisitos previos

En esta tarea se aprovisiona un pod de vSphere como host de salto para la conectividad SSH. Los pods de vSphere requieren redes de NSX-T para el clúster supervisor. Si utiliza redes de vDS para el clúster supervisor, utilice el siguiente método en su lugar: Conectarse mediante SSH a nodos de clúster de Tanzu Kubernetes como usuario del sistema con una contraseña.

Procedimiento

1 Conéctese al clúster supervisor.

   Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

2 Cree una variable de entorno denominada **`NAMESPACE`** cuyo valor sea el nombre del espacio de nombres de vSphere donde se aprovisiona el clúster de Tanzu Kubernetes de destino.

   ```
   export NAMESPACE=VSPHERE-NAMESPACE
   ```

3 Cambie el contexto a la instancia de espacio de nombres de vSphere en la que se aprovisiona el clúster de Tanzu Kubernetes.

   ```
   kubectl config use-context $NAMESPACE
   ```

4 Consulte el objeto secreto *`TKGS-CLUSTER-NAME`*`-ssh`.

   ```
   kubectl get secrets
   ```

5 Cree una instancia de pod de vSphere mediante las siguientes especificaciones `jumpbox.yaml`.

Reemplace el valor de `namespace` `YOUR-NAMESPACE` por el espacio de nombres de vSphere en el que se aprovisiona el clúster de destino. Reemplace el valor de `secretName` `YOUR-CLUSTER-NAME`-ssh con el nombre del clúster de destino.

```
apiVersion: v1
kind: Pod
metadata:
  name: jumpbox
  namespace: YOUR-NAMESPACE     #REPLACE
spec:
  containers:
  - image: "photon:3.0"
    name: jumpbox
    command: [ "/bin/bash", "-c", "--" ]
    args: [ "yum install -y openssh-server; mkdir /root/.ssh; cp /root/ssh/ssh-privatekey /
root/.ssh/id_rsa; chmod 600 /root/.ssh/id_rsa; while true; do sleep 30; done;" ]
    volumeMounts:
      - mountPath: "/root/ssh"
        name: ssh-key
        readOnly: true
    resources:
      requests:
        memory: 2Gi
  volumes:
    - name: ssh-key
      secret:
        secretName: YOUR-CLUSTER-NAME-ssh     #REPLACE
```

6 Implemente el pod aplicando la especificación `jumpbox.yaml`.

```
kubectl apply -f jumpbox.yaml
```

```
pod/jumpbox created
```

7 Compruebe que el pod se esté ejecutando.

```
kubectl get pods
```

```
NAME      READY   STATUS    RESTARTS   AGE
jumpbox   1/1     Running   0          3h9m
```

Nota También debe ver el pod de Jump Box en vCenter en el espacio de nombres de vSphere.

8 Cree una variable de entorno con la dirección IP del nodo de clúster de destino ejecutando el siguiente conjunto de comandos.

   a Obtenga el nombre de la máquina virtual de destino.

   ```
   kubectl get virtualmachines
   ```

   b Cree la variable de entorno `VMNAME` cuyo valor sea el nombre del nodo de destino.

   ```
   export VMNAME=NAME-OF-THE-VIRTUAL-MACHINE
   ```

   c Cree la variable de entorno `VMIP` cuyo valor sea la dirección IP de la máquina virtual del nodo de destino.

   ```
   export VMIP=$(kubectl -n $NAMESPACE get virtualmachine/$VMNAME -o
   jsonpath='{.status.vmIp}')
   ```

9 Para utilizar SSH en el nodo del clúster mediante el pod de Jump Box, ejecute el siguiente comando.

```
kubectl exec -it jumpbox  /usr/bin/ssh vmware-system-user@$VMIP
```

Importante La creación del contenedor e instalación del software tarda aproximadamente 60 segundos. Si recibe un "mensaje de error al ejecutar el comando en el contenedor: container_linux.go:370: starting container process caused: exec: "/usr/bin/ssh": stat /usr/bin/ssh: no such file or directory", vuelva a intentar el comando pasados unos segundos.

10 Para confirmar la autenticidad del host, introduzca **`yes`**.

```
The authenticity of host '10.249.0.999 (10.249.0.999)' can't be established.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.249.0.999' (ECDSA) to the list of known hosts.
Welcome to Photon 3.0
```

11 Confirme que ha iniciado sesión en el nodo de destino como `vmware-system-user`.

Por ejemplo, el siguiente resultado indica que ha iniciado sesión en un nodo del plano de control como usuario del sistema.

```
vmware-system-user@tkgs-cluster-1-control-plane-66tbr [ ~ ]$
```

12 Realice las operaciones deseadas en el nodo.

Atención Es posible que deba usar `sudo` o `sudo su` para realizar ciertas operaciones en el nodo, como reiniciar el kubelet.

13 Cuando termine, escriba **`exit`** para cerrar la sesión de SSH en pod de vSphere.

14 Para eliminar el pod, ejecute el comando `kubectl delete pod jumpbox`.

Precaución Por motivos de seguridad, considere la posibilidad de eliminar el pod de Jumpbox después de haber realizado su trabajo. Si es necesario, puede volver a crearla más adelante.

Conectarse mediante SSH a nodos de clúster de Tanzu Kubernetes como usuario del sistema con una contraseña

Puede conectarse mediante SSH a un nodo de clúster de Tanzu Kubernetes como `vmware-system-user` con una contraseña.

Puede conectarse a un nodo de clúster como usuario `vmware-system-user` con una contraseña. La contraseña se almacena como un secreto denominado `CLUSTER-NAME-ssh-password`. La contraseña está codificada en Base64 en `.data.ssh-passwordkey`. Puede proporcionar la contraseña a través de una sesión de SSH. Para obtener más información sobre este secreto, consulte Obtener los secretos del clúster de Tanzu Kubernetes.

Requisitos previos

Para enrutar las conexiones SSH en la red de cargas de trabajo adecuada, implemente una máquina virtual de host de salto de Linux en el entorno de vSphere en el que está habilitada **Administración de cargas de trabajo**. Consulte Crear una máquina virtual de host de salto de Linux.

Nota Se trata de un requisito estricto si desea conectarse a los nodos del clúster mediante SSH y utiliza redes de vDS, las cuales no admiten los pods de vSphere. También puede utilizar este enfoque con las redes de NSX-T si prefiere utilizar una contraseña en lugar de una clave privada para conectarse a través de SSH.

Procedimiento

1 Obtenga la dirección IP de la máquina virtual del host de salto, el nombre de usuario y la contraseña. Consulte Crear una máquina virtual de host de salto de Linux.

2 Conéctese al clúster supervisor.

   Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

3 Cambie el contexto al espacio de nombres de vSphere donde se aprovisiona el clúster de Tanzu Kubernetes de destino.

```
kubectl config use-context VSPHERE-NAMESPACE
```

4 Obtenga la dirección IP del nodo del clúster de destino.

   Enumere los nodos.

```
kubectl get virtualmachines
```

Describa los nodos para obtener la dirección IP del nodo de destino.

```
kubectl describe virtualmachines
```

5 Observe el secreto de `TKGS-CLUSTER-NAME-ssh-password`.

```
kubectl get secrets
```

6 Obtenga el valor de ssh-passwordkey para el clúster de destino.

```
kubectl get secrets TKGS-CLUSTER-NAME-ssh-password -o yaml
```

Por ejemplo, se devuelve ssh-passwordkey.

```
apiVersion: v1
data:
  ssh-passwordkey: RU1pQllLTC9TRjVFV0RBcCtmd1zwOTROeURYSWNGeXNReXJhaXRBUllYaz0=
```

7 Descodifique ssh-passwordkey.

El secreto está codificado en Base64. Para descodificarlo: en Linux, utilice `base64 --decode` (o `base64 -d`); en MacOS, utilice `base64 --Decode` (o `base64 -D`); en Windows, utilice una herramienta en línea.

```
echo <ssh-passwordkey> | base64 --decode
```

8 Conéctese mediante SSH al nodo del clúster de destino como `vmware-system-user`.

```
ssh vmware-system-user@TKGS-CLUSTER-NODE-IP-ADDRESS
```

9 Inicie sesión con la contraseña que descodificó.

Crear una máquina virtual de host de salto de Linux

Para utilizar SSH en los nodos del clúster de Tanzu Kubernetes con una contraseña, cree primero una máquina virtual de Jump Box que se conecte a la red de cargas de trabajo y la red de administración o front-end para la tunelización de SSH.

Crear una máquina virtual de host de salto de Linux

Siga estos pasos para crear una máquina virtual de Jump Box de Linux. Existen varias formas de hacerlo. Esta es una de ellas. Las instrucciones utilizan Photon OS, el cual se puede descargar aquí: https://github.com/vmware/photon/wiki/Downloading-Photon-OS.

1 Inicie sesión en vCenter Server con vSphere Client.

2 Cree una máquina virtual nueva.

3 Seleccione el sistema operativo invitado Linux, que en este ejemplo es VMware Photon OS (64 bits).

4 Instale el sistema operativo. Para ello, descargue el archivo ISO, asócielo a la máquina virtual e inícielo.

5 Configure la máquina virtual con una dirección IP en la red de cargas de trabajo.

6 Agregue una segunda NIC virtual a la máquina virtual y asígnela a la red de front-end.

7 Complete la configuración del sistema operativo y encienda la máquina virtual después de reiniciar.

8 Inicie sesión en la consola de vSphere de la máquina virtual como usuario raíz.

9 Cree una interfaz de red para la nueva NIC y asígnele una dirección IP en la red de front-end.

```
ifconfig eth1 IP-ADDRESS netmask NETMASK up
```

Nota Este método no es persistente durante los reinicios.

10 Compruebe que puede hacer ping en la puerta de enlace y el servidor DNS a través de esa interfaz.

11 En la consola de vSphere de la máquina virtual, configure un usuario de SSH con certificados. Para comprobar que funciona, cree un shell anidado.

12 Para verificar que funciona, ejecute SSH en Jump Box desde la red de front-end como el usuario de SSH.

13 Instale sshpass en la máquina virtual (de modo que pueda iniciar sesión a través de SSH con una contraseña). Para Photon OS, el comando es el siguiente:

```
tdnf install -y sshpass
```

14 Agregue la clave pública del cliente al archivo `~/.ssh/authorized_keys` y reinicie el proceso de `sshd` para que ssh pueda funcionar sin contraseña.

- Obtenga la clave pública, por ejemplo: `cat ~/.ssh/id_rsa.pub`.
- Acceda a la máquina virtual de jumphost.
- Cree el directorio SSH (si no existe): `mkdir -p ~/.ssh`.
- Anexe la clave pública al archivo `authorized_keys`: `echo ssh-rsa AAAA.... >> ~/.ssh/authorized_keys`. Reemplace `ssh-rsa AAAA....` por la cadena de clave pública completa que se obtuvo desde el comando `cat ~/.ssh/id_rsa.pub`.
- Asegúrese de que el directorio `~/.ssh` y el archivo `authorized_keys` tengan establecidos los permisos adecuados, por ejemplo: `chmod -R go= ~/.ssh`.

Conceder acceso de desarrollador a clústeres de Tanzu Kubernetes

Los desarrolladores son los usuarios de destino de Kubernetes. Una vez que se aprovisione un clúster de Tanzu Kubernetes, puede conceder acceso de desarrollador mediante autenticación de vCenter Single Sign-On.

Autenticación para desarrolladores

Un administrador de clústeres puede otorgar acceso al clúster a otros usuarios, como desarrolladores. Los desarrolladores pueden implementar pods en clústeres directamente mediante sus cuentas de usuario o de forma indirecta a través de cuentas de servicio. Para obtener más información, consulte Usar las directivas de seguridad de pods con clústeres de Tanzu Kubernetes.

- Para la autenticación de la cuenta de usuario, los clústeres de Tanzu Kubernetes admiten usuarios y grupos de vCenter Single Sign-On. El usuario o el grupo pueden ser locales para la instancia de vCenter Server o sincronizarse desde un servidor de directorio compatible.
- Para la autenticación de la cuenta de servicio, puede utilizar tokens de servicio. Para obtener más información, consulte la documentación de Kubernetes.

Agregar usuarios desarrolladores a un clúster

Para conceder acceso al clúster a desarrolladores, haga lo siguiente:

1. Defina una función o ClusterRole para el usuario o el grupo y aplíquelos al clúster. Para obtener más información, consulte la documentación de Kubernetes.
2. Cree un RoleBinding o ClusterRoleBinding para el usuario o grupo y aplíquelo al clúster. Vea el ejemplo siguiente:

Ejemplo de RoleBinding

Para conceder acceso a un usuario o grupo de vCenter Single Sign-On, el asunto en RoleBinding debe contener uno de los siguientes valores para el parámetro `name`.

Tabla 9-1. Campos de usuario y grupo admitidos

Campo	Descripción
`sso:`*`USER-NAME@DOMAIN`*	Por ejemplo, un nombre de usuario local, como `sso:joe@vsphere.local`.
`sso:`*`GROUP-NAME@DOMAIN`*	Por ejemplo, un nombre de grupo de un servidor de directorio integrado con la instancia de vCenter Server, como `sso:devs@ldap.example.com`.

El siguiente ejemplo de RoleBinding enlaza el usuario local de vCenter Single Sign-On, llamado Joe, al objeto ClusterRole predeterminado denominado `edit`. Esta función permite el acceso de lectura/escritura a la mayoría de los objetos en un espacio de nombres, en este caso, el espacio de nombres `default`.

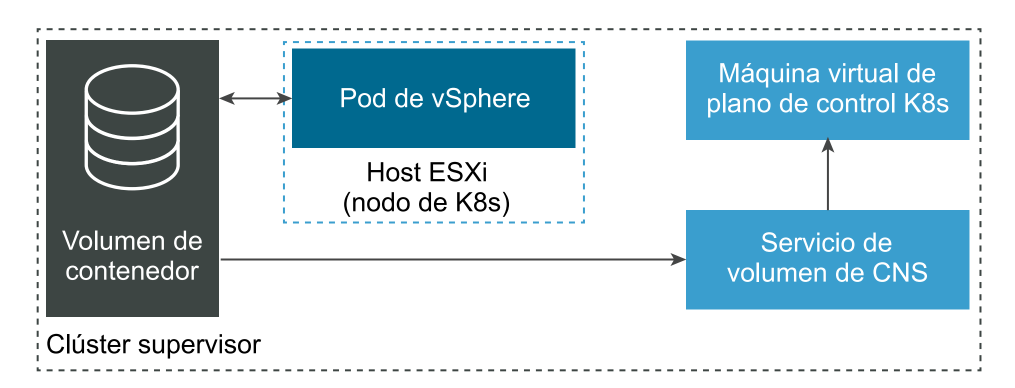
```
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: rolebinding-cluster-user-joe
  namespace: default
roleRef:
  kind: ClusterRole
  name: edit                             #Default ClusterRole
  apiGroup: rbac.authorization.k8s.io
subjects:
- kind: User
  name: sso:joe@vsphere.local            #sso:<username>@<domain>
  apiGroup: rbac.authorization.k8s.io
```

Usar almacenamiento persistente en vSphere with Tanzu

10

Ciertas cargas de trabajo de Kubernetes requieren almacenamiento persistente para almacenar datos de forma permanente. Para aprovisionar el almacenamiento persistente para cargas de trabajo de Kubernetes, la vSphere with Tanzu se integra con el almacenamiento nativo en la nube (Cloud Native Storage, CNS), un componente de vCenter Server que administra los volúmenes persistentes.

El almacenamiento persistente es utilizado por pods de vSphere, clústeres de Tanzu Kubernetes y máquinas virtuales. El siguiente ejemplo muestra cómo pod de vSphere utiliza el almacenamiento persistente.



Para comprender cómo funciona la vSphere with Tanzu con el almacenamiento persistente, familiarícese con los siguientes conceptos esenciales.

Volumen persistente

Para proporcionar almacenamiento persistente, Kubernetes utiliza volúmenes persistentes que pueden conservar su estado y sus datos. Si un pod monta volúmenes persistentes, estos siguen existiendo incluso cuando el pod se elimina o se vuelve a configurar. En el entorno de la vSphere with Tanzu, los objetos de volumen persistente están respaldados por los discos de primera clase en un almacén de datos.

La vSphere with Tanzu admite el aprovisionamiento dinámico y estático de volúmenes en modo de ReadWriteOnce, en donde los volúmenes se pueden montar mediante un solo pod.

A partir de vSphere 7.0 Update 3, vSphere with Tanzu también admite el modo ReadWriteMany para volúmenes persistentes en clústeres de Tanzu Kubernetes. Con la compatibilidad de ReadWriteMany, se puede montar un solo volumen simultáneamente mediante varios pods o aplicaciones que se ejecutan en un clúster. vSphere with Tanzu utiliza recursos compartidos de archivos de vSAN para volúmenes persistentes del tipo ReadWriteMany. Para obtener más información, consulte Crear volúmenes persistentes ReadWriteMany en vSphere with Tanzu.

Aprovisionamiento dinámico y estático

Con el aprovisionamiento dinámico de volúmenes, el almacenamiento no necesita ser aprovisionado previamente, y los volúmenes persistentes se pueden crear a pedido. Los ingenieros de desarrollo y operaciones emiten una notificación de volumen persistente que hace referencia a una clase de almacenamiento disponible en el espacio de nombres. vSphere with Tanzu aprovisiona automáticamente el volumen persistente correspondiente y un disco virtual de copia de seguridad.

Tanto el clúster supervisor como el clúster de Tanzu Kubernetes son compatibles con el aprovisionamiento dinámico.

Para obtener un ejemplo de cómo crear un volumen persistente de forma dinámica, consulte Aprovisionar un volumen persistente dinámico para una aplicación con estado.

Con el aprovisionamiento estático, puede utilizar un objeto de almacenamiento existente y ponerlo a disposición de un clúster.

Por lo general, un ingeniero de desarrollo y operaciones debe conocer los detalles del objeto de almacenamiento existente, las configuraciones admitidas y las opciones de montaje para poder reutilizarlo.

Para obtener un ejemplo de cómo aprovisionar un volumen persistente estático, consulte Aprovisionamiento de un volumen persistente estático en un clúster de Tanzu Kubernetes.

Disco de primera clase

vSphere with Tanzu usa el tipo de discos virtuales Disco de primera clase (FCD) para hacer copias de seguridad de volúmenes persistentes. El disco de primera clase, también conocido como "disco virtual mejorado", es un disco virtual con nombre que no está asociado con una máquina virtual.

Los discos de primera clase se identifican mediante UUID. Este UUID es globalmente único y es el identificador principal del FCD. El UUID sigue siendo válido incluso si el FCD se reubica o se genera una instantánea de él.

Notificación de volumen persistente

Los ingenieros de desarrollo y operaciones crean notificaciones de volumen persistente para solicitar recursos de almacenamiento persistentes. La solicitud aprovisiona un objeto de volumen persistente y un disco virtual coincidente. En vSphere Client, la notificación de volumen persistente se manifiesta como un disco virtual de FCD que pueden supervisar los administradores de vSphere.

La notificación está enlazada al volumen persistente. Las cargas de trabajo pueden utilizar la notificación para montar los volúmenes persistentes y acceder al almacenamiento.

Cuando los ingenieros de desarrollo y operaciones eliminan la notificación, también se eliminan el objeto de volumen persistente correspondiente y el disco virtual aprovisionado.

Clase de almacenamiento

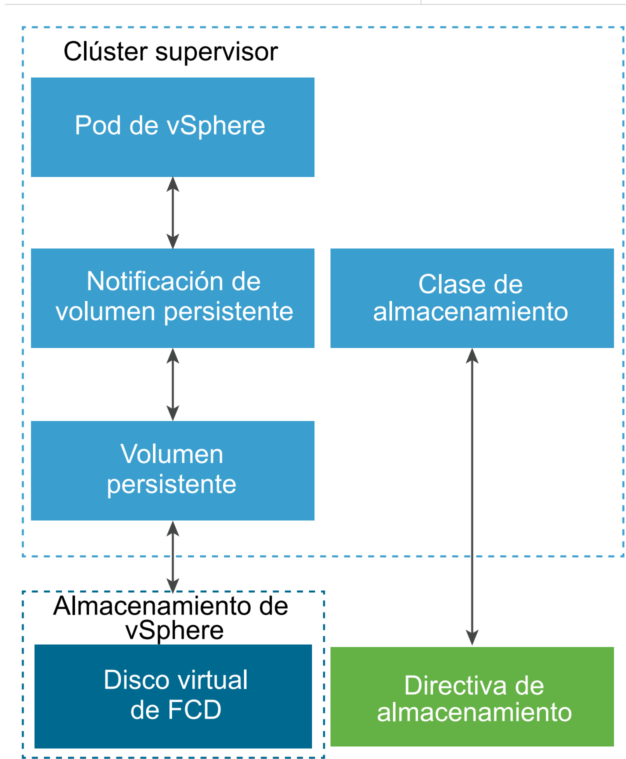
Kubernetes utiliza clases de almacenamiento para describir los requisitos de almacenamiento que respaldan los volúmenes persistentes. Los ingenieros de desarrollo y operaciones pueden incluir una clase de almacenamiento específica en su especificación de notificación de volumen persistente para solicitar el tipo de almacenamiento que describe la clase.

Flujo de trabajo de almacenamiento persistente

El flujo de trabajo para aprovisionar el almacenamiento persistente en vSphere with Tanzu generalmente incluye las siguientes acciones secuenciales.

Paso	Acción	Descripción
1	Los administradores de vSphere ofrecen recursos de almacenamiento persistentes al equipo de desarrollo y operaciones.	Los administradores de vSphere crean directivas de almacenamiento de máquina virtual que describen diferentes requisitos de almacenamiento y clases de servicios. A continuación, pueden asignar las directivas de almacenamiento a un espacio de nombres de vSphere.
2	La vSphere with Tanzu crea clases de almacenamiento que coinciden con las directivas de almacenamiento asignadas al espacio de nombres de vSphere.	Las clases de almacenamiento aparecen automáticamente en el entorno de Kubernetes, y el equipo de desarrollo y operaciones puede utilizarlas. Si un administrador de vSphere asigna varias directivas de almacenamiento al espacio de nombres de vSphere, se crea una clase de almacenamiento independiente para cada directiva de almacenamiento. Si utiliza servicio Tanzu Kubernetes Grid para aprovisionar clústeres de Tanzu Kubernetes, cada clúster de Tanzu Kubernetes heredará las clases de almacenamiento del espacio de nombres de vSphere en el que se aprovisiona el clúster.
3	Los ingenieros de desarrollo y operaciones utilizan las clases de almacenamiento para solicitar recursos de almacenamiento persistentes para una carga de trabajo.	La solicitud viene en forma de una notificación de volumen persistente que hace referencia a una clase de almacenamiento específica.

Paso	Acción	Descripción
4	vSphere with Tanzu crea un objeto de volumen persistente y un disco virtual persistente coincidente para una carga de trabajo.	vSphere with Tanzu coloca el disco virtual en el almacén de datos que cumple con los requisitos especificados en la directiva de almacenamiento original y su clase de almacenamiento correspondiente. El disco virtual puede montarse mediante una carga de trabajo.
5	Los administradores de vSphere supervisan los volúmenes persistentes en el entorno de la vSphere with Tanzu.	Mediante vSphere Client, los administradores de vSphere supervisan los volúmenes persistentes y sus discos virtuales de respaldo. También pueden supervisar el cumplimiento de almacenamiento y los estados de mantenimiento de los volúmenes persistentes.



Vea este vídeo para obtener información sobre el almacenamiento persistente en vSphere with Tanzu.

 (Almacenamiento persistente en vSphere with Kubernetes)

Tareas de administración de almacenamiento de un administrador de vSphere

Por lo general, las tareas de administración de almacenamiento persistente en vSphere with Tanzu incluyen lo siguiente. Como administrador de vSphere, utilice vSphere Client para realizar estas tareas.

- Realice operaciones de ciclo de vida de directivas de almacenamiento de máquina virtual.

  Antes de habilitar un clúster supervisor y configurar espacios de nombres, cree directivas de almacenamiento para el almacenamiento persistente. Las directivas de almacenamiento se basan en los requisitos de almacenamiento que le comunicaron los ingenieros de desarrollo y operaciones. Consulte Crear directivas de almacenamiento para vSphere with Tanzu.

  Nota No elimine la directiva de almacenamiento de vCenter Server ni del espacio de nombres de vSphere cuando se esté ejecutando una notificación de volumen persistente con la clase de almacenamiento correspondiente en el espacio de nombres. Esta recomendación también se aplica a los clústeres de Tanzu Kubernetes.

- Proporcione recursos de almacenamiento a los ingenieros de desarrollo y operaciones asignando las directivas de almacenamiento al espacio de nombres, y estableciendo límites de almacenamiento. Para obtener información sobre cómo cambiar las asignaciones de directivas de almacenamiento, consulte Cambiar la configuración de almacenamiento en un espacio de nombres. Para obtener información sobre la configuración de límites, consulte Configurar limitaciones en objetos de Kubernetes en un espacio de nombres de vSphere.
- Supervise los objetos de Kubernetes y su conformidad con la directiva de almacenamiento en vSphere Client. Consulte Supervisar volúmenes persistentes en vSphere Client.

Tareas de administración de almacenamiento de un ingeniero de desarrollo y operaciones

Por lo general, el ingeniero de desarrollo y operaciones utiliza `kubectl` para realizar las siguientes tareas de almacenamiento.

- Administre las clases de almacenamiento. Consulte Mostrar clases de almacenamiento en un espacio de nombres de vSphere o clúster de Tanzu Kubernetes.
- Implementar y administrar aplicaciones con estado. Consulte Aprovisionar un volumen persistente dinámico para una aplicación con estado.
- Realice operaciones de ciclo de vida para volúmenes persistentes. Ejemplos de notificación de volumen persistente de Tanzu Kubernetes.

Este capítulo incluye los siguientes temas:

- Cómo se integra vSphere with Tanzu con el almacenamiento de vSphere

- Funcionalidad admitida por el componente CNS-CSI de vSphere y CSI paravirtual en vSphere with Tanzu
- Permisos de almacenamiento en vSphere with Tanzu
- Crear directivas de almacenamiento para vSphere with Tanzu
- Cambiar la configuración de almacenamiento en el clúster supervisor
- Cambiar la configuración de almacenamiento en un espacio de nombres
- Mostrar clases de almacenamiento en un espacio de nombres de vSphere o clúster de Tanzu Kubernetes
- Aprovisionar un volumen persistente dinámico para una aplicación con estado
- Aprovisionamiento de un volumen persistente estático en un clúster de Tanzu Kubernetes
- Crear volúmenes persistentes ReadWriteMany en vSphere with Tanzu
- Expansión de volúmenes en vSphere with Tanzu
- Supervisar volúmenes persistentes en vSphere Client
- Supervisar el estado del volumen en un clúster de espacio de nombres de vSphere o Tanzu Kubernetes
- Usar la plataforma para la persistencia de datos de vSAN con servicios con estado modernos

Cómo se integra vSphere with Tanzu con el almacenamiento de vSphere

vSphere with Tanzu utiliza varios componentes para integrarse con el almacenamiento de vSphere.

Almacenamiento nativo en la nube (CNS) en vCenter Server

El componente CNS reside en vCenter Server. Se trata de una extensión de administración de vCenter Server que implementa las operaciones de aprovisionamiento y ciclo de vida de los volúmenes persistentes.

Cuando se aprovisionan volúmenes contenedores, el componente interactúa con la funcionalidad de disco de primera clase de vSphere para crear discos virtuales que respaldan dichos volúmenes. Adicionalmente, el componente de servidor de almacenamiento nativo en la nube se comunica con la administración de almacenamiento basada en directivas para garantizar un nivel necesario de servicio a los discos.

El almacenamiento nativo en la nube también realiza operaciones de consulta que permiten a los administradores de vSphere administrar y supervisar volúmenes persistentes y sus objetos de almacenamiento de respaldo a través de vCenter Server.

Disco de primera clase (First Class Disk, FCD)

También se denomina disco virtual mejorado. Se trata de un disco virtual designado que no está asociado con ninguna máquina virtual. Estos discos residen en un almacén de datos de VMFS, NFS o vSAN, y proporcionan respaldo a los volúmenes persistentes de ReadWriteOnce.

La tecnología FCD realiza operaciones de ciclo de vida relacionadas con volúmenes persistentes fuera de un ciclo de vida de una máquina virtual o un pod.

Al usar FCD, tenga en cuenta lo siguiente:

- Los FCD no admiten protocolos NFS 4.x. En su lugar, utilice NFS 3.
- vCenter Server no serializa las operaciones en el mismo FCD. Como resultado, las aplicaciones no pueden realizar operaciones simultáneamente en el mismo FCD. Realizar operaciones, tales como clonar, reubicar, eliminar, recuperar, etc., al mismo tiempo desde diferentes subprocesos provoca resultados impredecibles. Para evitar problemas, las aplicaciones deben realizar operaciones en el mismo FCD en un orden secuencial.
- FCD no es un objeto administrado y no admite un bloqueo global que proteja varias escrituras en un único FCD. Como resultado, FCD no admite varias instancias de vCenter Server que administren el mismo FCD. Si necesita utilizar varias instancias de vCenter Server con FCD, tiene las siguientes opciones:
  - Varias instancias de vCenter Server pueden administrar distintos almacenes de datos.
  - Varias instancias de vCenter Server no funcionan en el mismo FCD.

Administración de almacenamiento basada en directivas

La administración de almacenamiento basada en directivas es un servicio del vCenter Server que admite el aprovisionamiento de volúmenes persistentes y sus discos virtuales de respaldo según los requisitos de almacenamiento descritos en una directiva de almacenamiento. Después del aprovisionamiento, el servicio supervisa el cumplimiento del volumen con las características de directiva de almacenamiento. Para obtener más información sobre la administración basada en directivas de almacenamiento, consulte Administración basada en directivas de almacenamiento.

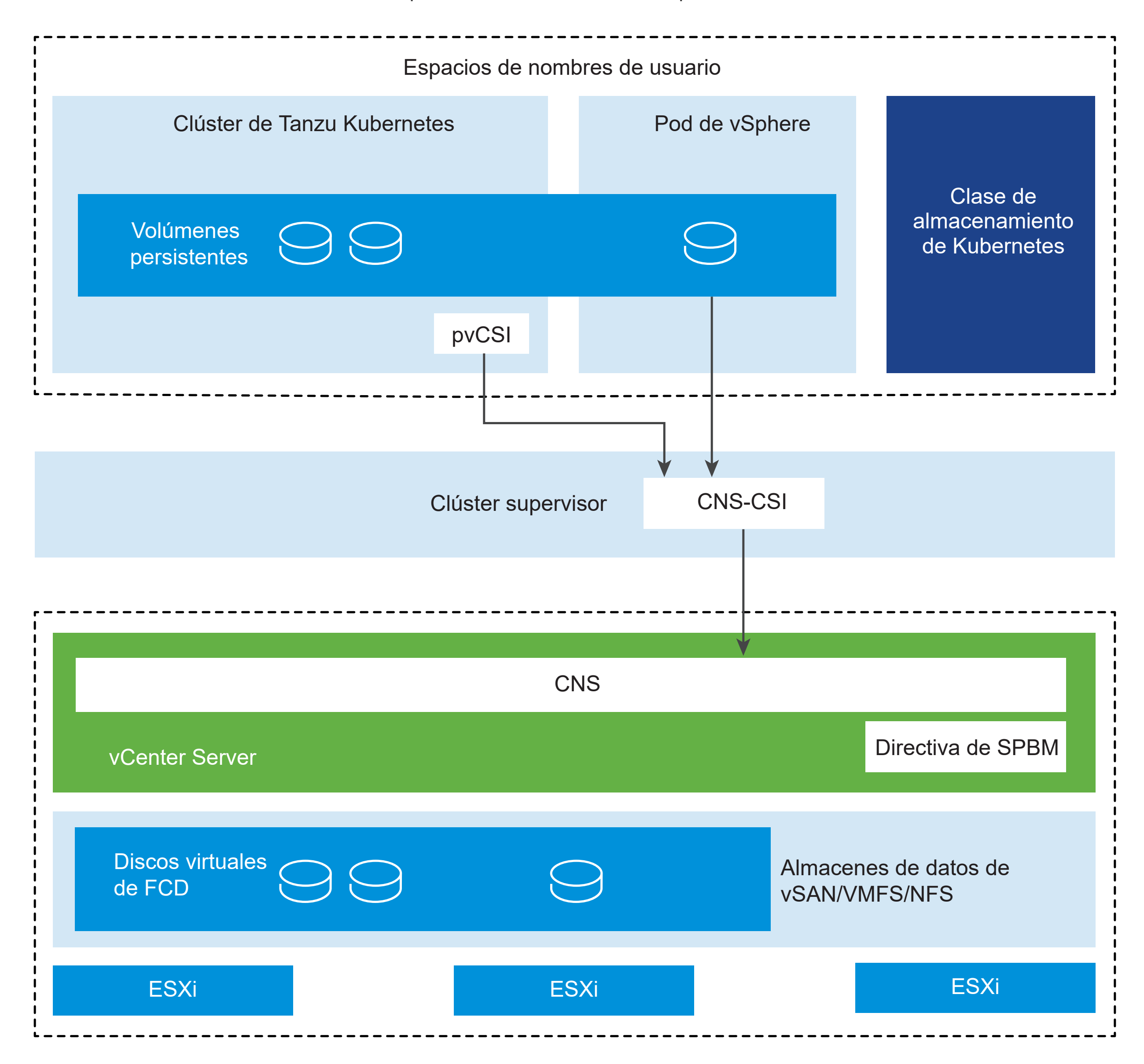
CNS-CSI de vSphere

El componente CNS-CSI de vSphere cumple con la especificación de la interfaz de almacenamiento de contenedor (Container Storage Interface, CSI), un estándar de la industria diseñado para proporcionar una interfaz que los orquestadores de contenedores como Kubernetes utilizan para aprovisionar el almacenamiento persistente. El controlador de CNS-CSI se ejecuta en clúster supervisor y conecta el almacenamiento de vSphere al entorno de Kubernetes en un espacio de nombres de vSphere. El componente CNS-CSI de vSphere se comunica directamente con el plano de control de CNS para todas las solicitudes de aprovisionamiento de almacenamiento provenientes de los pods de vSphere y los pods que se ejecutan en un clúster de Tanzu Kubernetes en el espacio de nombres.

CSI paravirtual (Paravirtual CSI, pvCSI)

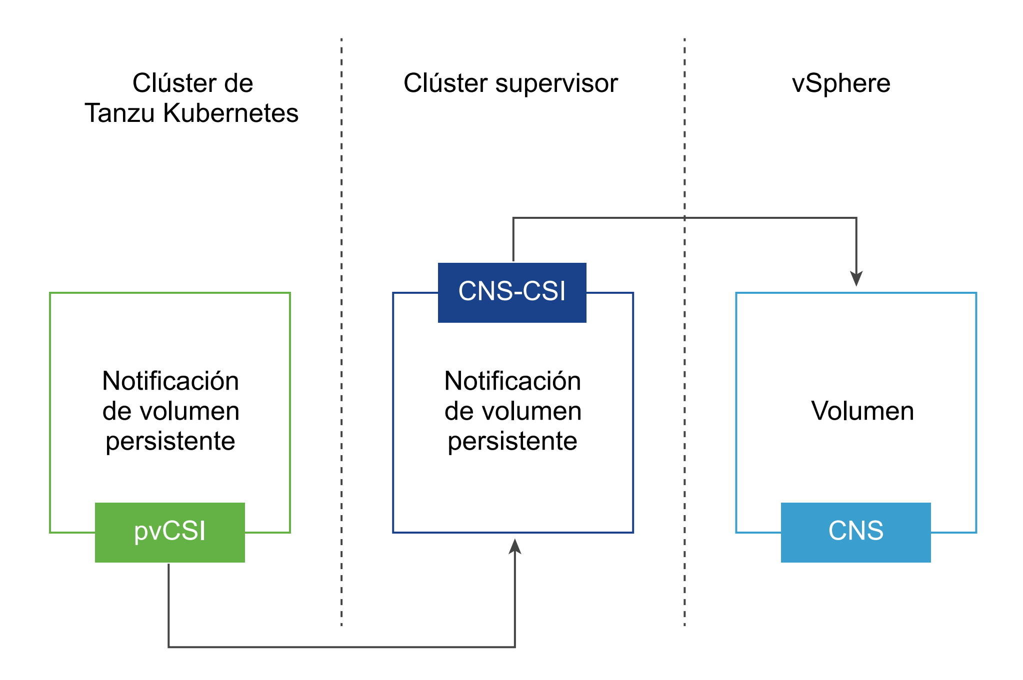
pvCSI es la versión del controlador de CNS-CSI vSphere modificada para los clústeres de Tanzu Kubernetes. pvCSI reside en el clúster de Tanzu Kubernetes y es responsable de todas las solicitudes relacionadas con el almacenamiento que se originan en el clúster de Tanzu Kubernetes. Las solicitudes se envían a CNS-CSI, que a su turno las propaga a CNS en vCenter Server. Como resultado, pvCSI no tiene comunicación directa con el componente de CNS, sino que depende del CNS-CSI para las operaciones de aprovisionamiento de almacenamiento.

A diferencia de CNS-CSI, pvCSI no requiere credenciales de infraestructura. Se configura con una cuenta de servicio en el espacio de nombres de vSphere.



A continuación, se muestra cómo interactúan diferentes componentes cuando un ingeniero de desarrollo y operaciones realiza una operación relacionada con el almacenamiento en el clúster de Tanzu Kubernetes, por ejemplo, crea una notificación de volumen persistente (Persistent Volume Claim, PVC).

El ingeniero de desarrollo y operaciones crea un PVC mediante la línea de comandos en el clúster de Tanzu Kubernetes. Esta acción genera un PVC que coincide en el clúster supervisor y activa el CNS-CSI. CNS-CSI invoca la API de creación de volumen de CNS.



Después de crear correctamente un volumen, la operación se propaga de vuelta a través del clúster supervisor al clúster de Tanzu Kubernetes. Como resultado de esta propagación, los usuarios pueden ver el volumen persistente y la notificación de volumen persistente en el estado enlazado en el clúster supervisor. Además, también verán el volumen persistente y la notificación de volumen persistente en el estado enlazado del clúster de Tanzu Kubernetes.

Funcionalidad admitida por el componente CNS-CSI de vSphere y CSI paravirtual en vSphere with Tanzu

El controlador del componente CNS-CSI de vSphere que se ejecuta en clúster supervisor y el controlador de pvCSI, que es la versión de CSI modificada para los clústeres de Tanzu Kubernetes, admiten varias funciones de almacenamiento de vSphere y Kubernetes. No obstante, se aplican algunas limitaciones.

Funcionalidades admitidas	CNS-CSI de vSphere con clúster supervisor	pvCSI con clúster de Tanzu Kubernetes
Compatibilidad de CNS en vSphere Client	Sí	Sí
Estado mejorado del objeto en vSphere Client	Sí (solo vSAN)	Sí (solo vSAN)
Volumen persistente de bloques dinámicos (modo de acceso ReadWriteOnce)	Sí	Sí

Funcionalidades admitidas	CNS-CSI de vSphere con clúster supervisor	pvCSI con clúster de Tanzu Kubernetes
Volumen persistente de archivos dinámicos (modo de acceso ReadWriteMany)	No	Sí (con Servicios de archivos de vSAN)
Almacén de datos de vSphere	VMFS/NFS/vSAN/vVols	VMFS/NFS/vSAN/vVols
Volumen persistente estático	Sí	Sí
Cifrado	No	No
Expansión de volumen sin conexión	Sí	Sí
Expansión de volumen conectado	Sí	Sí
Topologías de volumen y zonas	No	No
Varias instancias del plano de control de Kubernetes	Sí	Sí
WaitForFirstConsumer	No	No
VolumeHealth	Sí	Sí

Permisos de almacenamiento en vSphere with Tanzu

vSphere with Tanzu proporciona una función de muestra, administrador de almacenamiento de cargas de trabajo, que incluye un conjunto de privilegios para las operaciones de almacenamiento. Puede clonar esta función para crear una función similar.

Nombre del privilegio	Descripción	Necesario para
Cns.Permite búsquedas	Permite al administrador de almacenamiento ver la interfaz de usuario de almacenamiento nativo en la nube.	vCenter Server raíz
Almacén de datos.Asignar espacio **Almacén de datos.Operaciones de archivos de bajo nivel**	Permite asignar un espacio en un almacén de datos de una máquina virtual, una instantánea, un clon o un disco virtual. Permite realizar tareas de lectura, escritura, eliminación y cambio de nombre en el explorador del almacén de datos.	Almacén de datos compartido en el que residen volúmenes persistentes
ESX Agent Manager.Modificar	Permite modificar la máquina virtual de un agente, por ejemplo, apagar o eliminar la máquina virtual.	pod de vSphere
Recurso.Asignar máquina virtual a grupo de recursos	Permite asignar una máquina virtual a un grupo de recursos.	Grupos de recursos

Nombre del privilegio	Descripción	Necesario para
Almacenamiento basado en perfiles.Vista de almacenamiento basado en perfiles	Permite ver las directivas de almacenamiento definidas.	vCenter Server raíz
Máquina virtual.Cambiar configuración.Agregar un disco existente **Máquina virtual.Cambiar configuración.Agregar disco nuevo** **Máquina virtual.Cambiar configuración.Agregar o eliminar dispositivo** **Máquina virtual.Cambiar configuración.Cambiar ajustes** **Máquina virtual.Cambiar configuración.Eliminar disco** **Máquina virtual.Editar inventario.Crear nuevo** **Máquina virtual.Editar inventario.Eliminar**	Permite crear y eliminar máquinas virtuales. Permite configurar los dispositivos y las opciones de máquinas virtuales.	pod de vSphere

Crear directivas de almacenamiento para vSphere with Tanzu

Antes de habilitar vSphere with Tanzu, cree las directivas de almacenamiento que se utilizarán en el clúster supervisor y los espacios de nombres. Las directivas representan los almacenes de datos disponibles en el entorno de vSphere. Controlan la colocación de almacenamiento de objetos como las máquinas virtuales del plano de control, discos efímeros del pod, imágenes de contenedor y volúmenes de almacenamiento persistentes. Si utiliza clústeres de Tanzu Kubernetes, las directivas de almacenamiento también determinan cómo se implementan los nodos del clúster de Tanzu Kubernetes.

Según el entorno de almacenamiento de vSphere y las necesidades de desarrollo y operaciones, puede crear varias directivas de almacenamiento para representar diferentes clases de almacenamiento. Por ejemplo, si su entorno de almacenamiento de vSphere tiene tres clases de almacenes de datos (Bronce, Plata y Oro), puede crear directivas de almacenamiento para todos los almacenes de datos. Posteriormente, puede utilizar el almacén de datos Bronce para los discos virtuales efímeros y los discos virtuales de imagen de contenedor, y utilizar los almacenes de datos Plata y Oro para los discos virtuales de volumen persistente. Para obtener más información sobre las directivas de almacenamiento, consulte el capítulo Administración de almacenamiento basada en directivas de la documentación *Almacenamiento de vSphere*.

El siguiente ejemplo crea la directiva de almacenamiento para el almacén de datos etiquetado como Oro.

Si utiliza una plataforma persistencia de datos de vSAN, puede crear directivas de almacenamiento para almacenes de datos vSAN Direct o vSAN SNA. Para obtener información, consulte Crear directiva de almacenamiento de vSAN Direct y Crear directiva de almacenamiento SNA vSAN.

Requisitos previos

- Asegúrese de que el almacén de datos al que hace referencia en la directiva de almacenamiento se comparte entre todos los hosts de ESXi del clúster.
- Privilegios necesarios: **Directivas de almacenamiento de VM. Actualizar** y **Directivas de almacenamiento de VM. Ver**.

Procedimiento

1 Agregue etiquetas al almacén de datos.

   a Haga clic con el botón derecho en el almacén de datos que desea etiquetar y seleccione **Etiquetas y atributos personalizados > Asignar etiqueta**.

   b Haga clic en **Agregar etiqueta** y especifique las propiedades de la etiqueta.

Propiedad	Descripción
Nombre	Especifique el nombre de la etiqueta del almacén de datos, por ejemplo, `Oro`.
Descripción	Agregue la descripción de la etiqueta. Por ejemplo, `Almacén de datos para objetos de Kubernetes`.
Categoría	Seleccione una categoría existente o cree una categoría nueva. Por ejemplo, `Almacenamiento para Kubernetes`.

2 En vSphere Client, abra el asistente **Crear directiva de almacenamiento de máquina virtual**.

   a Haga clic en **Menú > Directivas y perfiles**.

   b En **Directivas y perfiles**, haga clic en **Directivas de almacenamiento de máquina virtual**.

   c Haga clic en **Crear directiva de almacenamiento de máquina virtual**.

3 Introduzca el nombre y la descripción de la directiva.

Opción	Acción
vCenter Server	Seleccione la instancia de vCenter Server.
Nombre	Introduzca el nombre de la directiva de almacenamiento (por ejemplo, **goldsp**). **Nota** Cuando vSphere with Tanzu convierte las directivas de almacenamiento que se asignan a espacios de nombres en clases de almacenamiento de Kubernetes, cambia todas las letras mayúsculas a minúsculas y reemplaza los espacios por guiones (-). Para evitar confusiones, utilice minúsculas y no use espacios en los nombres de las directivas de almacenamiento de máquina virtual.
Descripción	Introduzca la descripción de la directiva de almacenamiento.

4 En la página **Estructura de directiva** en **Reglas específicas de almacenes de datos**, habilite las reglas de ubicación basadas en etiquetas.

5 En la página **Colocación basada en etiquetas**, cree las reglas de la etiqueta.

Seleccione las opciones en función del siguiente ejemplo.

Opción	Descripción
Categoría de etiqueta	En el menú desplegable, seleccione la categoría de la etiqueta, por ejemplo, **Almacenamiento para Kubernetes**.
Opción de uso	Seleccione **Usar almacenamiento etiquetado con**.
Etiquetas	Haga clic en **Examinar etiquetas** y seleccione la etiqueta del almacén de datos, por ejemplo, **Oro**.

6 En la página **Compatibilidad de almacenamiento**, revise la lista de almacenes de datos que coinciden con esta directiva.

En este ejemplo, solo se muestra el almacén de datos etiquetado como Oro.

7 En la página **Revisar y finalizar**, revise la configuración de la directiva de almacenamiento y haga clic en **Finalizar**.

Resultados

Se mostrará la nueva directiva de almacenamiento para el almacén de datos etiquetado como Oro en la lista de directivas de almacenamiento existentes.

Pasos siguientes

Después de crear las directivas de almacenamiento, un administrador de vSphere puede realizar las siguientes tareas:

- Asignar las directivas de almacenamiento al clúster supervisor. Las directivas de almacenamiento configuradas en el clúster supervisor garantizan que las máquinas virtuales de plano de control, los discos efímeros del pod y las imágenes de contenedor se coloquen en los almacenes de datos que representan las directivas. Consulte Habilitar la administración de cargas de trabajo con redes de NSX-T Data Center.
- Asignar las directivas de almacenamiento al espacio de nombres de vSphere. Las directivas de almacenamiento visibles para el espacio de nombres determinan a qué almacenes de datos pueden acceder al espacio de nombres y cuáles pueden utilizar para los volúmenes persistentes. Las directivas de almacenamiento aparecen como clases de almacenamiento de Kubernetes coincidentes en el espacio de nombres. También se propagan al clúster de Tanzu Kubernetes en este espacio de nombres. Los ingenieros de desarrollo y operaciones pueden utilizar las clases de almacenamiento en sus especificaciones de notificación de volúmenes persistentes. Consulte Creación y configuración de un espacio de nombres de vSphere.

Cambiar la configuración de almacenamiento en el clúster supervisor

Las directivas de almacenamiento asignadas al clúster supervisor administran cómo se colocan los objetos como una máquina virtual de plano de control, el pod de vSphere y la memoria caché de imágenes de contenedor dentro de los almacenes de datos en el entorno de almacenamiento de vSphere. Por lo general, como administrador de vSphere debe configurar directivas de almacenamiento al habilitar el clúster supervisor. Si necesita realizar cambios en las asignaciones de directivas de almacenamiento después de la configuración inicial del clúster supervisor, realice esta tarea. También puede utilizar esta tarea para activar o desactivar la compatibilidad con volúmenes de archivos para volúmenes persistentes ReadWriteMany.

Los cambios que realice en la configuración de almacenamiento solo se aplican a los objetos nuevos.

Requisitos previos

Si tiene pensado activar la compatibilidad con volúmenes de archivos para volúmenes persistentes en el modo ReadWriteMany, siga los requisitos previos de Crear volúmenes persistentes ReadWriteMany en vSphere with Tanzu.

Procedimiento

1. En el vSphere Client, desplácese hasta el clúster de host que tiene vSphere with Tanzu habilitado.
2. Haga clic en la pestaña **Configurar** y, a continuación, haga clic en **Almacenamiento** dentro de **Espacio de nombres**.

3 Cambie las asignaciones de directivas de almacenamiento para los siguientes elementos.

Opción	Descripción
Nodo del plano de control	Seleccione la directiva de almacenamiento para la colocación de las máquinas virtuales del plano de control.
Discos efímeros del pod	Seleccione la directiva de almacenamiento para la colocación de los pods de vSphere.
Memoria caché de imágenes de contenedor	Seleccione la directiva de almacenamiento para la colocación de la memoria caché de las imágenes de contenedor.

4 Habilite la compatibilidad con volúmenes de archivos para implementar volúmenes persistentes ReadWriteMany.

Cambiar la configuración de almacenamiento en un espacio de nombres

Las directivas de almacenamiento que un administrador de vSphere asigna a un espacio de nombres en una instancia de clúster supervisor controlan la forma en la que se colocan los volúmenes persistentes y los nodos del clúster de Tanzu Kubernetes en los almacenes de datos de vSphere. Las notificaciones de volumen persistente que corresponden a volúmenes persistentes pueden provenir de un pod de vSphere o un clúster de Tanzu Kubernetes. Puede cambiar las asignaciones de directivas de almacenamiento originales.

Requisitos previos

Antes de eliminar una directiva de almacenamiento del vCenter Server o de un espacio de nombres de vSphere, o de cambiar la asignación de la directiva de almacenamiento, asegúrese de que no haya ninguna notificación de volumen persistente con la clase de almacenamiento correspondiente en el espacio de nombres. Asimismo, asegúrese de que ningún clúster de Tanzu Kubernetes esté utilizando la clase de almacenamiento.

Procedimiento

1 En el vSphere Client, navegue al espacio de nombres.

   a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

   b Haga clic en la pestaña **Espacios de nombres** y haga clic en el espacio de nombres.

2 Haga clic en la pestaña **Almacenamiento** y, a continuación, en **Directivas de almacenamiento**.

3 Haga clic en el icono **Editar** para cambiar las asignaciones de directivas de almacenamiento.

Mostrar clases de almacenamiento en un espacio de nombres de vSphere o clúster de Tanzu Kubernetes

Después de que el administrador de vSphere crea una directiva de almacenamiento y la asigna al espacio de nombres de vSphere, la directiva de almacenamiento se muestra como una clase

de almacenamiento de Kubernetes coincidente en el espacio de nombres y los clústeres de Tanzu Kubernetes disponibles. Como ingeniero de desarrollo y operaciones, puede comprobar que la clase de almacenamiento esté disponible.

Su habilidad para ejecutar los comandos depende de sus permisos.

Requisitos previos

Asegúrese de que el administrador de vSphere haya creado una directiva de almacenamiento adecuada y haya asignado la directiva al espacio de nombres de vSphere.

Procedimiento

1 Utilice uno de los siguientes comandos para comprobar que las clases de almacenamiento estén disponibles.

- **`kubectl get storageclass`**

  Nota Este comando solo está disponible para los usuarios con privilegios de administrador.

  Obtendrá un resultado similar al siguiente: El nombre de la clase de almacenamiento coincide con el nombre de la Directiva de almacenamiento en el lado de vSphere.

  ```
  NAME      PROVISIONER             AGE
  silver    csi.vsphere.vmware.com  2d
  gold      csi.vsphere.vmware.com  1d
  ```

- **`kubectl describe namespace`** ***namespace_name***

  En el resultado, el nombre de la clase de almacenamiento aparece como parte del parámetro ***storageclass_name*****.storageclass.storage.k8s.io/requests.storage**. Por ejemplo:

  ```
  -----------------
  Name:                                                              namespace_name
   Resource                                                           Used  Hard
   --------                                                           ---   ---
   silver.storageclass.storage.k8s.io/requests.storage                1Gi
  9223372036854775807
   gold.storageclass.storage.k8s.io/requests.storage                  0
  9223372036854775807
  ```

2 Para comprobar la cantidad de espacio de almacenamiento disponible en el espacio de nombres, ejecute el siguiente comando.

   `kubectl describe resourcequotas -namespace` ***namespace***

Obtendrá un resultado similar al siguiente:

```
Name:              ns-my-namespace
Namespace:         ns-my-namespace
Resource           Used  Hard
--------           ----  ----
requests.storage   0     200Gi
```

Aprovisionar un volumen persistente dinámico para una aplicación con estado

Las aplicaciones con estado (por ejemplo, bases de datos) guardan datos entre sesiones y requieren almacenamiento persistente para almacenar los datos. Estos datos que se conservan se denominan estado de la aplicación. Posteriormente, puede recuperarlos y utilizarlos en la siguiente sesión. Kubernetes ofrece volúmenes persistentes como objetos que pueden conservar su estado y sus datos.

En el entorno de vSphere, los objetos de volúmenes persistentes se respaldan con discos virtuales que residen en almacenes de datos. Los almacenes de datos se representan a través de directivas de almacenamiento. Después de que el administrador de vSphere crea una directiva de almacenamiento (por ejemplo, **`Oro`**) y la asigna a un espacio de nombres en un clúster supervisor, la directiva de almacenamiento se muestra como una clase de almacenamiento de Kubernetes coincidente en el espacio de nombres de vSphere y los clústeres de Tanzu Kubernetes disponibles.

Como ingeniero de desarrollo y operaciones, puede utilizar la clase de almacenamiento en sus especificaciones de notificación de volúmenes persistentes. Posteriormente, puede implementar una aplicación que utilice almacenamiento de la notificación de volumen persistente. En este ejemplo, el volumen persistente de la aplicación se crea de forma dinámica.

Requisitos previos

Asegúrese de que el administrador de vSphere haya creado una directiva de almacenamiento adecuada y haya asignado la directiva al espacio de nombres.

Procedimiento

1 Acceda al espacio de nombres en el entorno de Kubernetes de vSphere.

2 Compruebe que las clases de almacenamiento se encuentren disponibles.

   Consulte Mostrar clases de almacenamiento en un espacio de nombres de vSphere o clúster de Tanzu Kubernetes.

3 Cree una notificación de volumen persistente (Persistent Volume Claim, PVC).

a Cree un archivo YAML que contenga la configuración de notificación de volumen persistente.

En este ejemplo, el archivo hace referencia a la clase de almacenamiento **gold**.

Para aprovisionar un volumen persistente ReadWriteMany, establezca `accessModes` en `ReadWriteMany`. Consulte Crear volúmenes persistentes ReadWriteMany en vSphere with Tanzu.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: gold
  resources:
    requests:
        storage: 3Gi
```

b Aplique la notificación de volumen persistente al clúster de Kubernetes.

```
kubectl apply -f pvc_name.yaml
```

Este comando crea de forma dinámica un volumen persistente de Kubernetes y un volumen de vSphere con un disco virtual de respaldo que cumple los requisitos de almacenamiento de la notificación.

c Compruebe el estado de la notificación de volumen persistente.

```
kubectl get pvc my-pvc
```

El resultado muestra que el volumen está enlazado a la notificación de volumen persistente.

```
NAME     STATUS    VOLUME   CAPACITY   ACCESSMODES   STORAGECLASS   AGE
my-pvc   Bound     my-pvc   2Gi        RWO           gold           30s
```

4 Cree un pod que monte el volumen persistente.

a Cree un archivo YAML que incluya el volumen persistente.

El archivo contiene estos parámetros.

```
...
volumes:
    - name: my-pvc
      persistentVolumeClaim:
        claimName: my-pvc
```

b Implemente el pod desde el archivo YAML.

```
kubectl create -f pv_pod_name.yaml
```

c Compruebe que se haya creado el pod.

```
kubectl get pod
```

```
NAME        READY   STATUS    RESTARTS   AGE
pod_name    1/1     Ready     0          40s
```

Resultados

El pod que configuró utilizará el almacenamiento persistente que se describe en la notificación de volumen persistente.

Pasos siguientes

Para supervisar el estado de mantenimiento del volumen persistente, consulte Supervisar el estado del volumen en un clúster de espacio de nombres de vSphere o Tanzu Kubernetes. Para revisar y supervisar el volumen persistente en vSphere Client, consulte Supervisar volúmenes persistentes en vSphere Client.

Aprovisionamiento de un volumen persistente estático en un clúster de Tanzu Kubernetes

Puede crear estáticamente un volumen de bloque en un clúster de Tanzu Kubernetes mediante una notificación de volumen persistente (PVC) sin utilizar desde el clúster supervisor.

La PVC debe cumplir las siguientes condiciones:

- Estar presente en el mismo espacio de nombres en el que reside el clúster de Tanzu Kubernetes.
- No estar asociada a un pod de vSphere en el clúster supervisor ni a un pod en cualquier clúster de Tanzu Kubernetes.

Con el aprovisionamiento estático, también puede reutilizar en un nuevo clúster de Tanzu Kubernetes una PVC que ya no necesite otro clúster de Tanzu Kubernetes. Para ello, cambie la `Reclaim policy` del volumen persistente (PV) en el clúster de Tanzu Kubernetes original a `Retain` y, a continuación, elimine la PVC correspondiente.

Siga estos pasos para crear estáticamente una PVC en un nuevo clúster de Tanzu Kubernetes utilizando la información del volumen subyacente de sobra.

Procedimiento

1 Anote el nombre de la PVC original en el clúster supervisor.

   Si vuelve a utilizar la PVC de un clúster de Tanzu Kubernetes antiguo, puede recuperar el nombre de la PVC de `volumeHandle` del objeto PV anterior del clúster de Tanzu Kubernetes.

2 Crear un PV.

   En el archivo YAML, especifique los valores de los siguientes elementos:

   - Para `storageClassName`, puede introducir el nombre de la clase de almacenamiento que utiliza su PVC en el clúster supervisor.
   - Para `volumeHandle`, introduzca el nombre de PVC que obtuvo en Step 1.

   Si está reusando un volumen de otro clúster de Tanzu Kubernetes, elimine los objetos de PVC y PV del clúster de Tanzu Kubernetes anterior antes de crear un PV en el nuevo clúster de Tanzu Kubernetes.

   Utilice el siguiente manifiesto de YAML como ejemplo.

```
apiVersion: v1
   kind: PersistentVolume
   metadata:
     name: static-tkg-block-pv
     annotations:
       pv.kubernetes.io/provisioned-by: csi.vsphere.vmware.com
   spec:
     storageClassName: gc-storage-profile
     capacity:
       storage: 2Gi
     accessModes:
       - ReadWriteOnce
     persistentVolumeReclaimPolicy: Delete
     claimRef:
       namespace: default
       name: static-tkg-block-pvc
     csi:
       driver: "csi.vsphere.vmware.com"
       volumeAttributes:
         type: "vSphere CNS Block Volume"
       volumeHandle: "supervisor-block-pvc-name"  # Enter the PVC name from the Supervisor
cluster.
```

3 Cree un PVC para que coincida con el objeto PV que creó en el paso 2.

Establezca la `storageClassName` en el mismo valor que en el PV.

```
kind: PersistentVolumeClaim
   apiVersion: v1
   metadata:
     name: static-tkg-block-pvc
   spec:
     accessModes:
       - ReadWriteOnce
     resources:
       requests:
         storage: 2Gi
     storageClassName: gc-storage-profile
     volumeName: static-tkg-block-pv
```

4 Compruebe que la PVC esté enlazada al PV que creó.

```
$ kubectl get pv,pvc
 NAME                                   CAPACITY   ACCESS MODES   RECLAIM POLICY
STATUS   CLAIM                         STORAGECLASS         REASON   AGE
 persistentvolume/static-tkg-block-pv    2Gi        RWO            Delete
Bound    default/static-tkg-block-pvc   gc-storage-profile            10s

 NAME                                         STATUS   VOLUME                 CAPACITY
ACCESS MODES   STORAGECLASS         AGE
 persistentvolumeclaim/static-tkg-block-pvc   Bound    static-tkg-block-pv   2Gi
RWO            gc-storage-profile   10s
```

Crear volúmenes persistentes ReadWriteMany en vSphere with Tanzu

A partir de la versión vSphere 7.0 Update 3, vSphere with Tanzu admite volúmenes persistentes en modo ReadWriteMany. Con la compatibilidad de ReadWriteMany, se puede montar un solo volumen simultáneamente mediante varios pods o aplicaciones que se ejecutan en un clúster. vSphere with Tanzu utiliza servicios de archivos de vSAN para proporcionar recursos compartidos de archivos para los volúmenes persistentes ReadWriteMany.

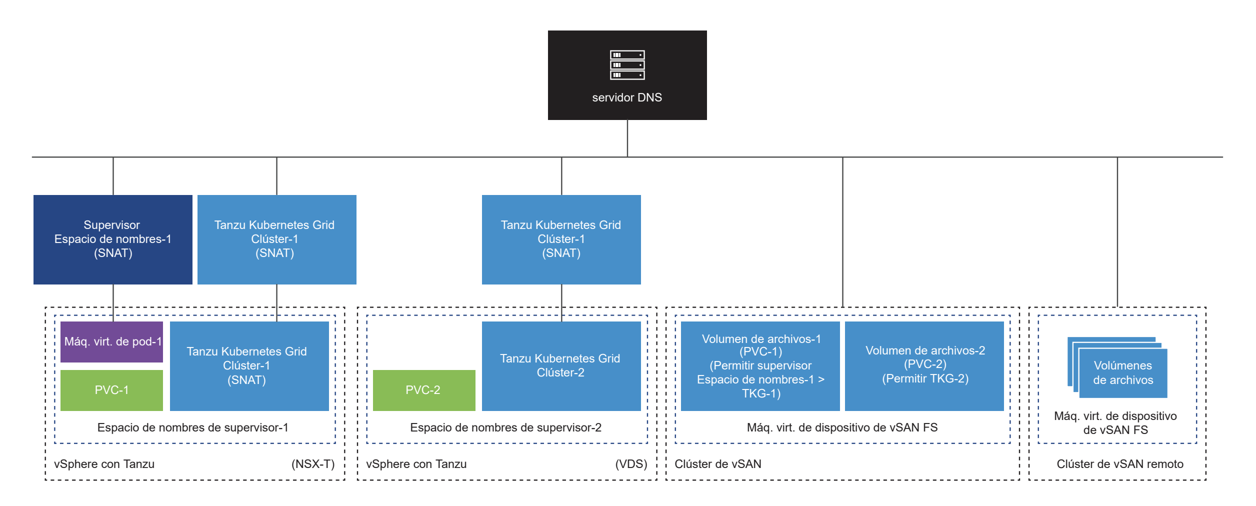
Consideraciones para los volúmenes persistentes ReadWriteMany

Cuando habilite la compatibilidad con ReadWriteMany para volúmenes persistentes en vSphere with Tanzu, tenga en cuenta las siguientes consideraciones.

- Con los clústeres de Tanzu Kubernetes, utilice la versión 1.22 de Tkr.

  Nota Solo puede utilizar la funcionalidad ReadWriteMany cuando se publique la próxima versión 1.22 de Tkr. Para obtener información sobre las versiones de TKr, consulte las notas de la versión de VMware Tanzu Kubernetes.

- Cuando habilite la compatibilidad con volúmenes de archivos para vSphere with Tanzu, tenga en cuenta las posibles debilidades de seguridad:
  - Los volúmenes se montan sin cifrado. Es posible acceder a los datos sin cifrar mientras los datos transitan por la red.
  - Se utilizan listas de control de acceso (ACL) para que los recursos compartidos de archivos aíslen la capacidad de acceso a ellos dentro de un espacio de nombres de supervisor. Puede tener riesgo de suplantación de IP.
- Siga estas directrices para redes:
  - Asegúrese de que espacio de nombres de vSphere esté en modo NAT. Consulte Creación y configuración de un espacio de nombres de vSphere.
  - Compruebe que los servicios de archivos de vSAN se puedan enrutar desde la red de carga de trabajo y que no haya ninguna NAT entre la red de carga de trabajo y las direcciones IP de servicios de archivos de vSAN.
  - Utilice un servidor DNS común para los servicios de archivos de vSAN y el clúster de vSphere.



- Si después de habilitar la compatibilidad con volúmenes de archivos, la desactiva más adelante, los volúmenes persistentes ReadWriteMany existentes que aprovisionó en el clúster no se verán afectados y se podrán seguir usando. No podrá crear nuevos volúmenes persistentes de ReadWriteMany.

Flujo de trabajo para habilitar la compatibilidad con ReadWriteMany para volúmenes persistentes

Siga este proceso para habilitar la compatibilidad con ReadWriteMany para volúmenes persistentes.

1 Un administrador de vSphere configura un clúster de vSAN con servicios de archivos de vSAN configurados. Consulte Configurar servicios de archivos.

2 Un administrador de vSphere activa la compatibilidad con volúmenes de archivos en clúster supervisor.

Acción	Descripción
Active la compatibilidad con volúmenes de archivos al habilitar la plataforma Administración de cargas de trabajo.	■ Habilitar la administración de cargas de trabajo con redes de vSphere ■ Habilitar la administración de cargas de trabajo con redes de NSX-T Data Center
Active la compatibilidad con volúmenes de archivos en el clúster existente, por ejemplo, después de una actualización de vSphere with Tanzu.	Cambiar la configuración de almacenamiento en el clúster supervisor

3 Un ingeniero de desarrollo y operaciones aprovisiona un volumen persistente que configura la PVC `accessMode` como `ReadWriteMany`.

Se pueden aprovisionar varios pods con la misma PVC.

Consulte Aprovisionar un volumen persistente dinámico para una aplicación con estado.

Expansión de volúmenes en vSphere with Tanzu

Como ingeniero de desarrollo y operaciones, puede utilizar la función de expansión de volúmenes de Kubernetes para expandir un volumen de bloque persistente una vez creado. Ambos tipos de clústeres, tanto clústeres supervisor como de Tanzu Kubernetes, admiten la expansión de volúmenes en línea y sin conexión.

De forma predeterminada, las clases de almacenamiento que aparecen en el entorno de vSphere with Tanzu tienen `allowVolumeExpansion` establecido en `true`. Gracias a este parámetro, es posible modificar el tamaño de un volumen en línea y sin conexión.

Se considera que un volumen está sin conexión cuando no está asociado a un nodo o pod. Un volumen en línea es un volumen disponible en un nodo o pod.

El nivel de compatibilidad de la funcionalidad de expansión de volúmenes depende de la versión de vSphere. Puede expandir los volúmenes creados en las versiones anteriores de vSphere cuando actualice el entorno de vSphere a las versiones adecuadas que admitan las ampliaciones.

Si utiliza un clúster de Tanzu Kubernetes, asegúrese de actualizar tanto el clúster de Tanzu Kubernetes como el clúster supervisor a la versión adecuada para que la funcionalidad se admita. La funcionalidad en el clúster de Tanzu Kubernetes depende de la habilitación de esa característica en el clúster supervisor.

Por ejemplo, si actualiza el clúster de Tanzu Kubernetes a vSphere 7.0 Update 2 y deja el clúster supervisor en la versión 7.0 Update 1, la expansión de volúmenes en línea no funcionará en el clúster de Tanzu Kubernetes.

	clúster supervisor 7.0	clúster supervisor 7.0 Update 1	clúster supervisor 7.0 Update 2
Clúster de Tanzu Kubernetes 7.0	Expansiones en línea y sin conexión en un clúster de Tanzu Kubernetes o un clúster supervisor: `not supported`	Expansiones en línea y sin conexión en un clúster de Tanzu Kubernetes o un clúster supervisor: `not supported`	■ Expansiones en línea y sin conexión en un clúster de Tanzu Kubernetes: `not supported` ■ Expansiones en línea y sin conexión en un clúster supervisor: `supported`
Clúster de Tanzu Kubernetes 7.0 Update 1	Expansiones en línea y sin conexión en un clúster de Tanzu Kubernetes o un clúster supervisor: `not supported`	■ Expansión sin conexión en un clúster de Tanzu Kubernetes: `supported` ■ Expansión sin conexión en un clúster supervisor: `not supported` ■ Expansión en línea en un clúster de Tanzu Kubernetes o un clúster supervisor: `not supported`	■ Expansión sin conexión en un clúster de Tanzu Kubernetes: `supported` ■ Expansión en línea en un clúster de Tanzu Kubernetes: `not supported` ■ Expansiones en línea y sin conexión en un clúster supervisor: `supported`
Clúster de Tanzu Kubernetes 7.0 Update 2	Expansiones en línea y sin conexión en un clúster de Tanzu Kubernetes o un clúster supervisor: `not supported`	■ Expansión sin conexión en un clúster de Tanzu Kubernetes: `supported` ■ Expansión sin conexión en un clúster supervisor: `not supported` ■ Expansión en línea en un clúster de Tanzu Kubernetes o un clúster supervisor: `not supported`	Expansiones en línea y sin conexión en un clúster de Tanzu Kubernetes o un clúster supervisor: `supported`

Al expandir los volúmenes, tenga en cuenta lo siguiente:

- Puede expandir los volúmenes hasta los límites especificados por las cuotas de almacenamiento. vSphere with Tanzu admite solicitudes de cambio de tamaño consecutivas para un objeto de notificación de volumen persistente.
- Todos los tipos de almacenes de datos, incluidos VMFS, vSAN, vSAN Direct, vVols y NFS, admiten la expansión de volúmenes.
- Puede realizar una expansión de volúmenes para implementaciones o pods independientes.
- Puede cambiar el tamaño de los volúmenes aprovisionados estáticamente en un clúster supervisor y un clúster de Tanzu Kubernetes si los volúmenes tienen clases de almacenamiento asociadas.
- No puede expandir volúmenes creados como parte de StatefulSet.

- Si un disco virtual que crea una copia de seguridad de un volumen tiene instantáneas, no se puede cambiar su tamaño.
- vSphere with Tanzu no admite la expansión de volúmenes para volúmenes en un árbol o migrados.

Expandir un volumen persistente en modo sin conexión

Se considera que un volumen está sin conexión cuando no está asociado a un nodo o pod. Ambos tipos de clústeres, los clústeres clústeres supervisor y Tanzu Kubernetes, admiten la expansión de volúmenes sin conexión.

Requisitos previos

Asegúrese de actualizar el entorno de vSphere a una versión adecuada que admita la expansión de volúmenes sin conexión. Consulte Expansión de volúmenes en vSphere with Tanzu.

Procedimiento

1 Cree una notificación de volumen persistente (PVC) con una clase de almacenamiento.

   a Defina una PVC con el siguiente manifiesto de YAML como ejemplo.

   En el ejemplo, el tamaño del almacenamiento solicitado es 1 Gi.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: example-block-pvc
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: example-block-sc
```

   b Aplique la PVC al clúster de Kubernetes.

```
kubectl apply -f example-block-pvc.yaml
```

2 Aplique una revisión a la PVC para aumentar su tamaño.

   Si la PVC no está asociado a un nodo o no lo está usando un pod, utilice el siguiente comando para aplicar una revisión a la PVC. En este ejemplo, el aumento de almacenamiento solicitado es de 2 Gi.

```
kubectl patch pvc example-block-pvc -p '{"spec": {"resources": {"requests": {"storage": "2Gi"}}}}'
```

   Con esta acción se activa una expansión en el volumen asociado a la PVC.

3 Compruebe que el tamaño del volumen haya aumentado.

```
kubectl get pv
NAME                                       CAPACITY ACCESS MODES RECLAIM POLICY STATUS
CLAIM                       STORAGECLASS           REASON AGE
pvc-9e9a325d-ee1c-11e9-a223-005056ad1fc1   2Gi           RWO          Delete      Bound
default/example-block-pvc   example-block-sc              6m44s
```

Nota El tamaño de la PVC no cambia hasta que un pod utiliza la PVC.

El siguiente ejemplo muestra que el tamaño de la PVC no ha cambiado. Si describe la PVC, puede ver la condición `FilesystemResizePending` aplicada en la PVC.

```
kubectl get pvc
NAME                STATUS VOLUME                                     CAPACITY ACCESS
MODES   STORAGECLASS       AGE
example-block-pvc   Bound  pvc-9e9a325d-ee1c-11e9-a223-005056ad1fc1   1Gi
RWO       example-block-sc   6m57s
```

4 Cree un pod para utilizar la PVC.

Cuando el pod utiliza la PVC, se expande el sistema de archivos.

5 Compruebe que el tamaño de la PVC se haya modificado.

```
kubectl get pvc
NAME                STATUS VOLUME                                    CAPACITY ACCESS MODES
STORAGECLASS     AGE
example-block-pvc   Bound  pvc-24114458-9753-428e-9c90-9f568cb25788   2Gi          RWO
example-block-sc 2m12s
```

La condición `FilesystemResizePending` se ha eliminado de la PVC. La expansión del volumen se ha completado.

Pasos siguientes

Un administrador de vSphere puede ver el nuevo tamaño del volumen en vSphere Client. Consulte Supervisar volúmenes persistentes en vSphere Client.

Expandir un volumen persistente en modo en línea

Un volumen en línea es un volumen disponible en un nodo o pod. Como ingeniero de desarrollo y operaciones, puede expandir un volumen de bloque persistente en línea. Ambos tipos de clústeres, clústeres supervisor y Tanzu Kubernetes, admiten la expansión de volúmenes en línea.

Requisitos previos

Asegúrese de actualizar el entorno de vSphere a una versión adecuada que admita la expansión de volúmenes en línea. Consulte Expansión de volúmenes en vSphere with Tanzu.

Procedimiento

1 Busque la notificación de volumen persistente para cambiar el tamaño.

```
$ kubectl get pv,pvc,pod
NAME                                                        CAPACITY   ACCESS MODES
RECLAIM POLICY   STATUS      CLAIM               STORAGECLASS   REASON   AGE
persistentvolume/pvc-5cd51b05-245a-4610-8af4-f07e77fdc984   1Gi        RWO
Delete           Bound       default/block-pvc   block-sc                 4m56s

NAME                              STATUS   VOLUME
CAPACITY   ACCESS MODES   STORAGECLASS   AGE
persistentvolumeclaim/block-pvc   Bound    pvc-5cd51b05-245a-4610-8af4-f07e77fdc984
1Gi        RWO            block-sc       5m3s

NAME             READY   STATUS    RESTARTS   AGE
pod/block-pod   1/1     Running   0          26s
```

Tenga en cuenta que el tamaño del almacenamiento que utiliza el volumen es de 1 Gi.

2 Aplique una revisión a la PVC para aumentar su tamaño.

Por ejemplo, aumente el tamaño a 2 Gi.

```
$ kubectl patch pvc block-pvc -p '{"spec": {"resources": {"requests": {"storage":
"2Gi"}}}}'
persistentvolumeclaim/block-pvc edited
```

Con esta acción se activa una expansión en el volumen asociado a la PVC.

3 Compruebe que el tamaño de PVC y PV haya aumentado.

```
$ kubectl get pvc,pv,pod
NAME                              STATUS   VOLUME
CAPACITY   ACCESS MODES   STORAGECLASS   AGE
persistentvolumeclaim/block-pvc   Bound    pvc-5cd51b05-245a-4610-8af4-f07e77fdc984
2Gi        RWO            block-sc       6m18s

NAME                                                        CAPACITY   ACCESS MODES
RECLAIM POLICY   STATUS      CLAIM               STORAGECLASS   REASON   AGE
persistentvolume/pvc-5cd51b05-245a-4610-8af4-f07e77fdc984   2Gi        RWO
Delete           Bound       default/block-pvc   block-sc                 6m11s

NAME             READY   STATUS    RESTARTS   AGE
pod/block-pod   1/1     Running   0          101s
```

Pasos siguientes

Un administrador de vSphere puede ver el nuevo tamaño del volumen en vSphere Client. Consulte Supervisar volúmenes persistentes en vSphere Client.

Supervisar volúmenes persistentes en vSphere Client

Cuando los ingenieros de desarrollo y operaciones implementan una aplicación con estado que contiene una notificación de volumen persistente, la vSphere with Tanzu crea un objeto de volumen persistente y un disco virtual persistente coincidente. Como administrador de vSphere, puede revisar los detalles del volumen persistente en vSphere Client. También puede supervisar el estado de mantenimiento y el cumplimiento de almacenamiento.

Procedimiento

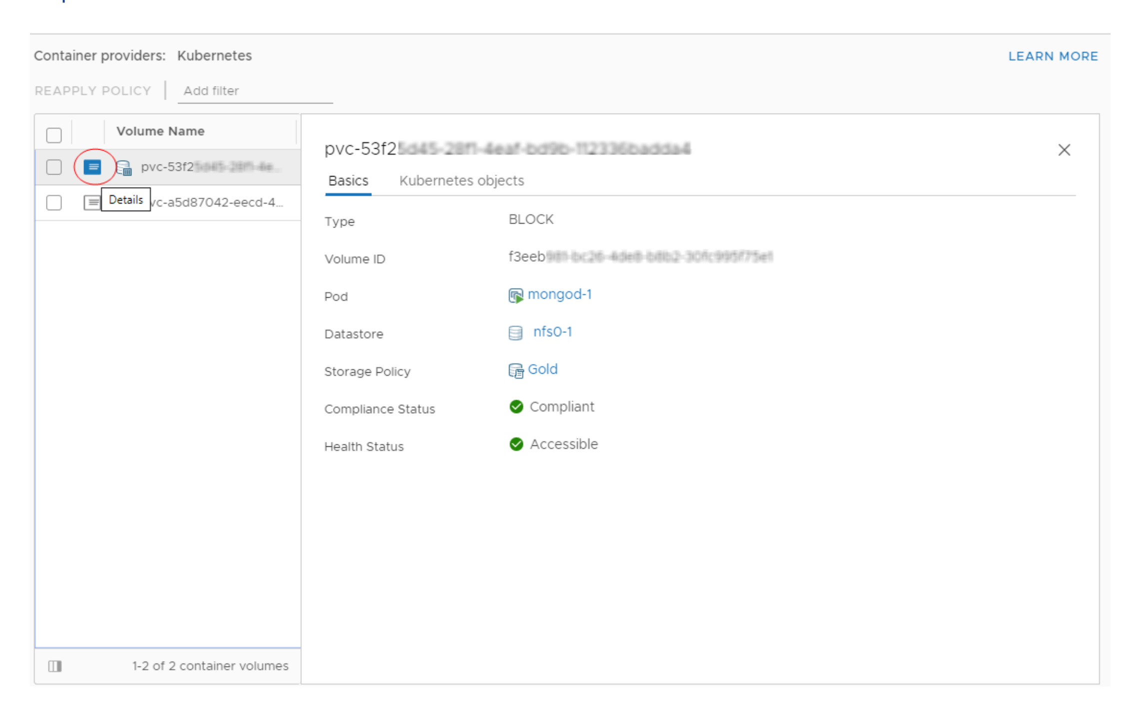
1. En vSphere Client, desplácese hasta el espacio de nombres que tiene los volúmenes persistentes.
   a. En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.
   b. Haga clic en el espacio de nombres.
2. Haga clic en la pestaña **Almacenamiento** y, a continuación, en **Notificaciones de volumen persistente**.

   En vSphere Client, se enumeran todos los objetos de notificación de volumen persistente y los volúmenes correspondientes disponibles en el espacio de nombres.
3. Para ver los detalles de una notificación de volumen persistente seleccionada, haga clic en el nombre del volumen en la columna **Nombre de volumen persistente**.

4 En la página **Volúmenes contenedores**, compruebe el estado de mantenimiento del volumen y el cumplimiento de la directiva de almacenamiento.

a Haga clic en el icono **Detalles** y alterne entre las pestañas **Conceptos básicos** y **Objetos de Kubernetes** para ver información adicional sobre el volumen persistente de Kubernetes.

Para supervisar el estado de mantenimiento del volumen con el comando `kubectl`, consulte Supervisar el estado del volumen en un clúster de espacio de nombres de vSphere o Tanzu Kubernetes.



b Compruebe el estado de mantenimiento del volumen.

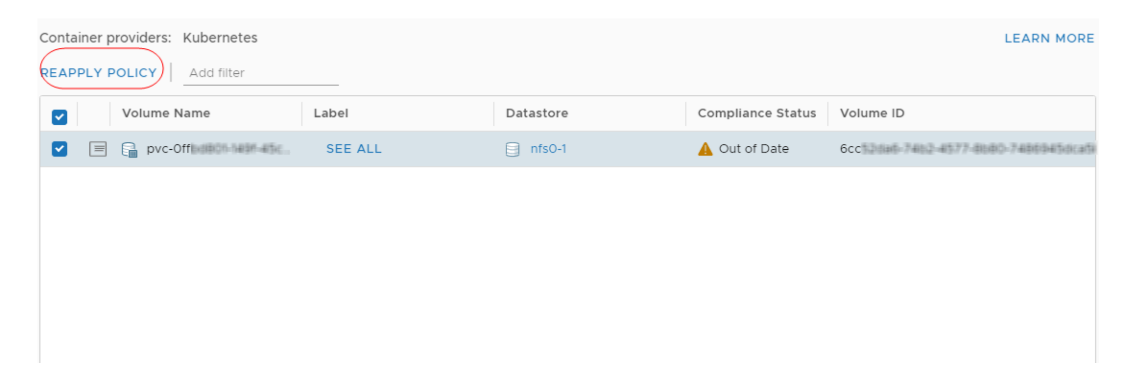
Estado de mantenimiento	Descripción
Accesible	Puede accederse al volumen persistente y está disponible para su uso.
Inaccesible	No puede accederse al volumen persistente y no puede usarse. El volumen persistente se vuelve inaccesible si los hosts que se conectan al almacén de datos no pueden acceder al almacén de datos que almacena el volumen.

c Compruebe el estado de cumplimiento del almacenamiento.

Puede ver una de las siguientes opciones en la columna **Estado de cumplimiento**.

Estado de cumplimiento	Descripción
Conforme	El almacén de datos donde reside el disco virtual de respaldo del volumen tiene las capacidades de almacenamiento que requiere la directiva.
Desactualizado	Este estado indica que la directiva se editó, pero no se comunicaron los nuevos requisitos de almacenamiento al almacén de datos. Para comunicar los cambios, vuelva a aplicar la directiva en el volumen desactualizado.
No compatible	El almacén de datos cumple con los requisitos de almacenamiento especificados, pero actualmente no puede cumplir con la directiva de almacenamiento. Por ejemplo, el estado puede ser de no cumplimiento cuando los recursos físicos del almacén de datos no están disponibles. Puede lograr que el almacén de datos cumpla con los requisitos si realiza cambios en la configuración física del clúster de hosts, por ejemplo, si agrega hosts o discos al clúster. Si los recursos adicionales cumplen con la directiva de almacenamiento, el estado pasará a ser Cumplimiento.
No aplicable	La directiva de almacenamiento hace referencia a las capacidades del almacén de datos no admitidas por el almacén de datos.

d Si el estado de cumplimiento es Desactualizado, seleccione el volumen y haga clic en **Volver a aplicar directiva**.



El estado pasará a ser Conforme.

Supervisar el estado del volumen en un clúster de espacio de nombres de vSphere o Tanzu Kubernetes

Como ingeniero de desarrollo y operaciones, puede comprobar el estado de mantenimiento de un volumen persistente en un estado enlazado.

Para cada volumen persistente en un estado enlazado, el estado de mantenimiento aparece en el campo `Annotations: volumehealth.storage.kubernetes.io/messages:` de la notificación de volumen persistente enlazada al volumen persistente. Existen dos valores posibles para el estado de mantenimiento.

Estado de mantenimiento	Descripción
Accesible	Puede accederse al volumen persistente y está disponible para su uso.
Inaccesible	No puede accederse al volumen persistente y no puede usarse. El volumen persistente se vuelve inaccesible si los hosts que se conectan al almacén de datos no pueden acceder al almacén de datos que almacena el volumen.

Para supervisar el estado de mantenimiento del volumen en vSphere Client, consulte Supervisar volúmenes persistentes en vSphere Client.

Procedimiento

1 Acceda al espacio de nombres en el entorno de Kubernetes de vSphere.

2 Cree una notificación de volumen persistente (Persistent Volume Claim, PVC).

   a Cree un archivo YAML que contenga la configuración de notificación de volumen persistente.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: gold
  resources:
    requests:
        storage: 2Gi
```

   b Aplique la notificación de volumen persistente al clúster de Kubernetes.

```
kubectl apply -f pvc_name.yaml
```

   Este comando crea un volumen persistente de Kubernetes y un volumen de vSphere con un disco virtual de respaldo que cumple con los requisitos de almacenamiento de la notificación.

   c Compruebe si la notificación de volumen persistente está enlazada a un volumen.

```
kubectl get pvc my-pvc
```

   El resultado muestra que la notificación de volumen persistente y el volumen se encuentran enlazados.

```
NAME     STATUS    VOLUME    CAPACITY   ACCESSMODES   STORAGECLASS   AGE
my-pvc   Bound     my-pvc    2Gi        RWO           gold           30s
```

3 Compruebe el estado de mantenimiento del volumen.

Ejecute el siguiente comando para comprobar la anotación del estado del volumen de la notificación de volumen persistente enlazada al volumen persistente.

```
kubectl describe pvc my-pvc
```

En los siguientes resultados de ejemplo, el campo `volumehealth.storage.kubernetes.io/messages` muestra el estado de mantenimiento como accesible.

```
Name:           my-pvc
Namespace:      test-ns
StorageClass:   gold
Status:         Bound
Volume:         my-pvc
Labels:         <none>
Annotations:    pv.kubernetes.io/bind-completed: yes
                pv.kubernetes.io/bound-by-controller: yes
                volume.beta.kubernetes.io/storage-provisioner: csi.vsphere.vmware.com
                volumehealth.storage.kubernetes.io/messages: accessible
Finalizers:     [kubernetes.io/pvc-protection]
Capacity:       2Gi
Access Modes:   RWO
VolumeMode:     Filesystem
```

Usar la plataforma para la persistencia de datos de vSAN con servicios con estado modernos

Puede utilizar la plataforma para la persistencia de datos de vSAN para servicios con estado modernos que requieren almacenamiento persistente. La plataforma proporciona un marco que permite a terceros integrar sus aplicaciones de servicio con la infraestructura de vSphere subyacente, de modo que el software de terceros pueda ejecutarse en vSphere with Tanzu de forma óptima.

Entre las ventajas de usar la persistencia de datos de vSAN se incluyen las siguientes:

Implementación y ampliación automáticas de servicios

Con vSphere Client, los administradores pueden instalar e implementar un servicio con estado moderno en un clúster supervisor y conceder acceso al espacio de nombres del servicio a los ingenieros de desarrollo y operaciones. Los ingenieros de desarrollo y operaciones pueden aprovisionar y ampliar instancias del servicio con estado de forma dinámica como si fuera un autoservicio a través de las API de Kubernetes.

Supervisión de servicios integrada con vCenter Server

Los partners pueden crear complementos de paneles de control que se integren con vCenter Server. Con estos complementos de interfaz de usuario, los administradores de vSphere

pueden administrar y supervisar los servicios con estado. Además, vSAN ofrece funciones de supervisión de estado y capacidad para estos servicios de terceros integrados.

Configuración de almacenamiento optimizada con vSAN Direct

vSAN Direct habilita los servicios con estado moderno para que se conecten directamente con el almacenamiento de conexión directa subyacente y, de este modo, optimizar la eficiencia de E/S y el almacenamiento.

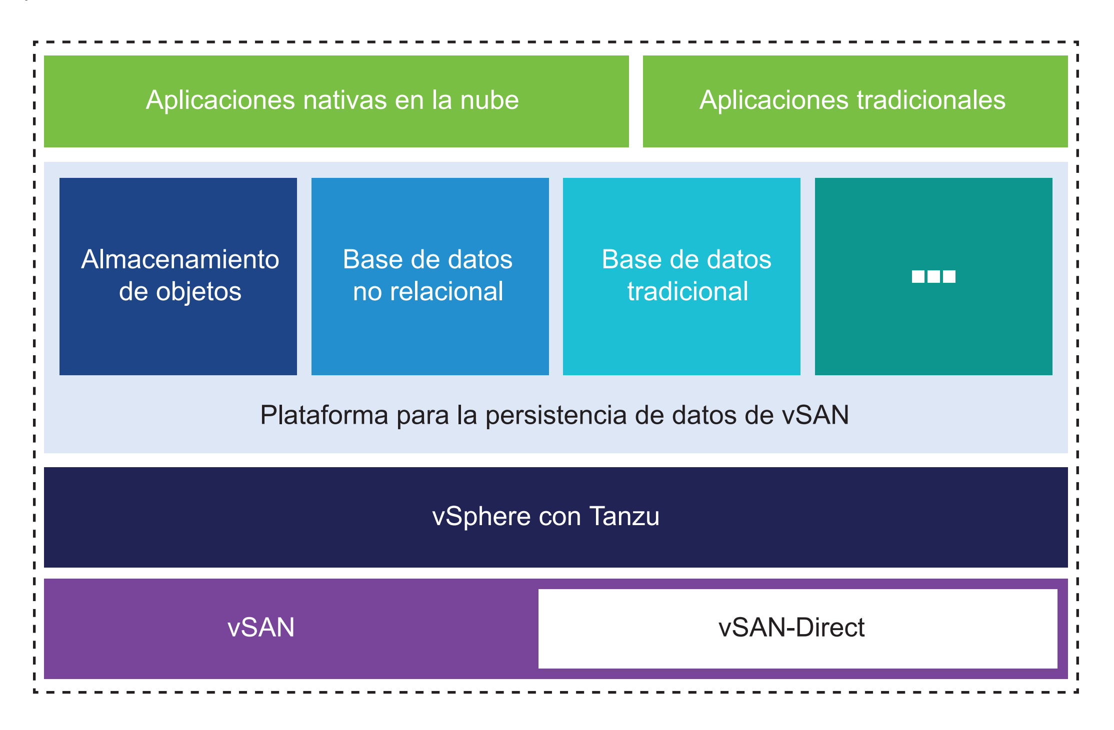
La plataforma admite los siguientes tipos de servicios:

- Almacenamiento de objetos, como MinIO.
- Las bases de datos de NoSQL, también denominadas bases de datos no relacionales.
- Bases de datos tradicionales.

Almacenamiento que no comparte nada de vSphere

La mayoría de servicios con estado modernos tienen una arquitectura de no compartir nada (Shared Nothing Architecture, SNA). Consumen almacenamiento local no replicado y ofrecen sus propios servicios de replicación de almacenamiento, compresión y otras operaciones de datos. Como resultado, los servicios no aprovechan que las mismas operaciones se hayan ya realizado en el almacenamiento subyacente.

Para evitar duplicar las operaciones, la plataforma para la persistencia de datos de vSAN ofrece dos soluciones vSAN con rutas de datos optimizadas. El servicio persistente puede entonces ejecutarse en vSAN con la directiva de almacenamiento de SNA o en un almacenamiento local prácticamente sin formato denominado vSAN Direct.



vSAN con la directiva de almacenamiento de SNA

Con esta tecnología, puede usar un almacén de datos de vSAN replicado distribuido con la directiva de SNA de host local vSAN. Como resultado, la aplicación del servicio de SNA puede controlar la colocación y asumir la responsabilidad de mantener disponibles los datos. Con la tecnología, al servicio persistente le resulta más fácil coubicar su instancia de recurso informático y un objeto de almacenamiento en el mismo host ESXi físico. Con la colocación de host-local, es posible realizar operaciones como la replicación en la capa de servicio y no en la capa de almacenamiento.

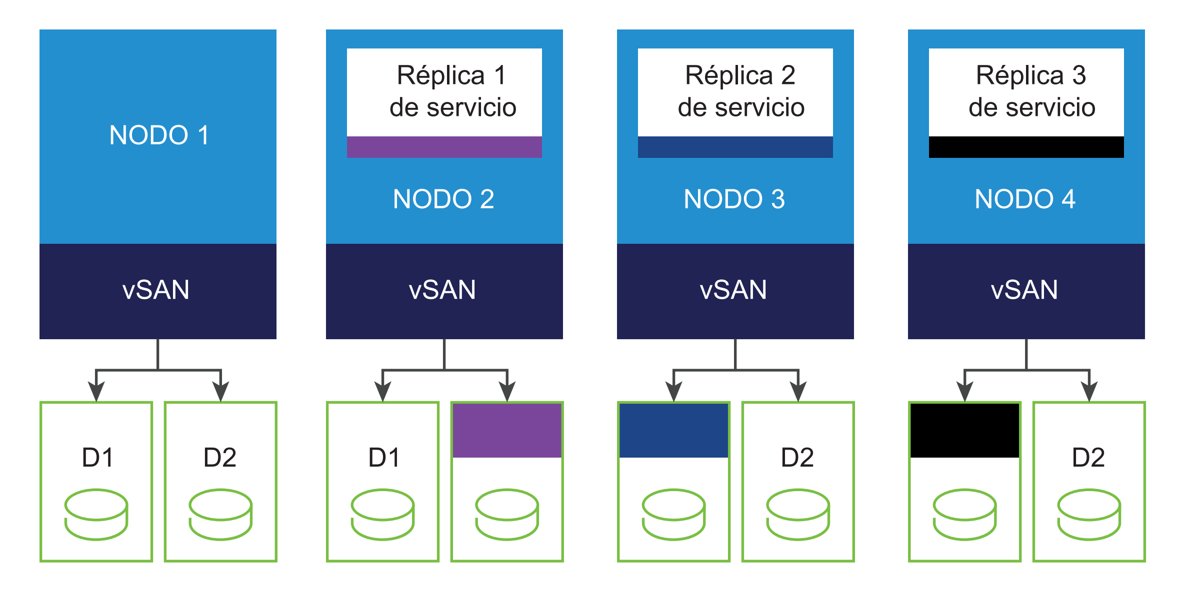
La instancia de recurso informático, como un pod, aparece primero en uno de los nodos del clúster de vSAN. A continuación, el objeto de vSAN creado con la directiva de SNA de vSAN tendrá automáticamente todos los datos colocados en el mismo nodo en el que se ejecuta el pod.

En el siguiente ejemplo se muestra la implementación de almacenamiento de una aplicación que utiliza la clase de almacenamiento de SNA para su volumen persistente. vSAN puede seleccionar cualquier grupo de discos en el nodo para la colocación de volúmenes persistentes.

Total de copias de datos = 3

Tolerancia a errores esperada = 2

Errores reales que se toleran de forma garantizada = 2

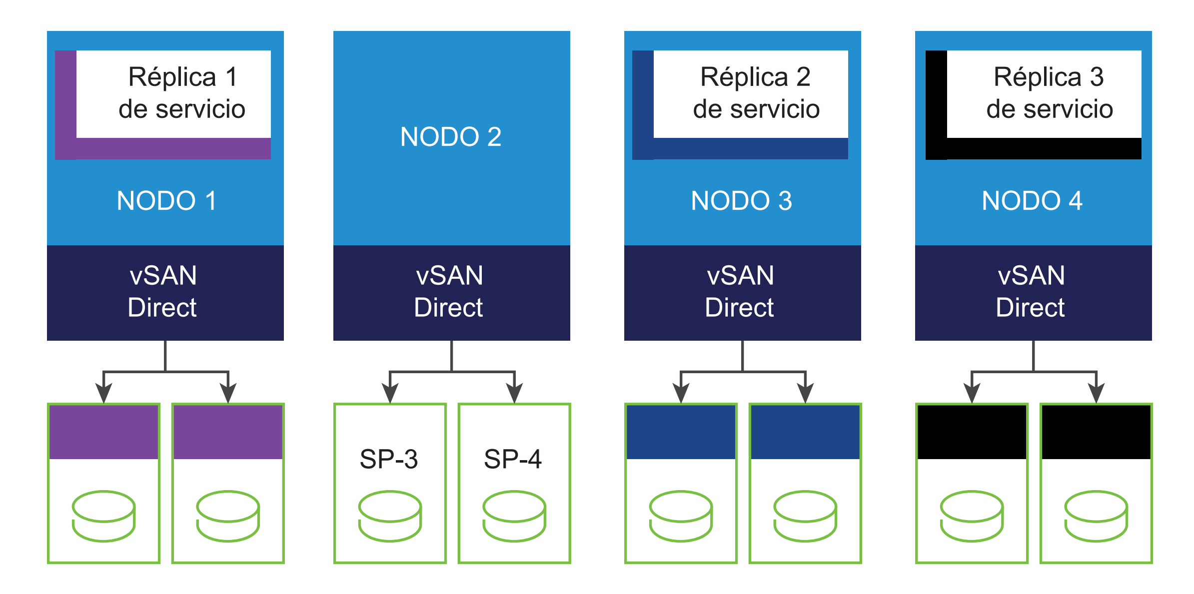


vSAN Direct

A pesar de que vSAN con la directiva de almacenamiento de SNA pueden colocar datos de forma local en la instancia de recurso informático, existe una sobrecarga de una ruta de datos de vSAN distribuida entre la aplicación y el dispositivo de almacenamiento físico. Con vSAN Direct, las aplicaciones de servicios con estado pueden acceder en su mayoría al almacenamiento local sin formato de vSAN a través de una ruta de acceso de datos más directa, la cual ofrece la solución optimizada de mayor rendimiento.

Con vSAN Direct, el administrador de vSphere puede reclamar dispositivos de host-local y, a continuación, administrar y supervisar los dispositivos. vSAN Direct proporciona información sobre el estado, el rendimiento y la capacidad de los dispositivos. En cada dispositivo local que reclama, vSAN Direct crea un almacén de datos de VMFS independiente y lo pone a disposición de la aplicación como una opción de colocación. Los almacenes de datos de VMFS que administra vSAN Direct se muestran como grupos de almacenamiento en Kubernetes. En vSphere Client, aparecen como almacenes de datos de vSAN Direct.

A continuación se muestran los volúmenes persistentes colocados en local en los discos de vSAN Direct.



Cuándo hay que utilizar vSAN con SNA o vSAN Direct

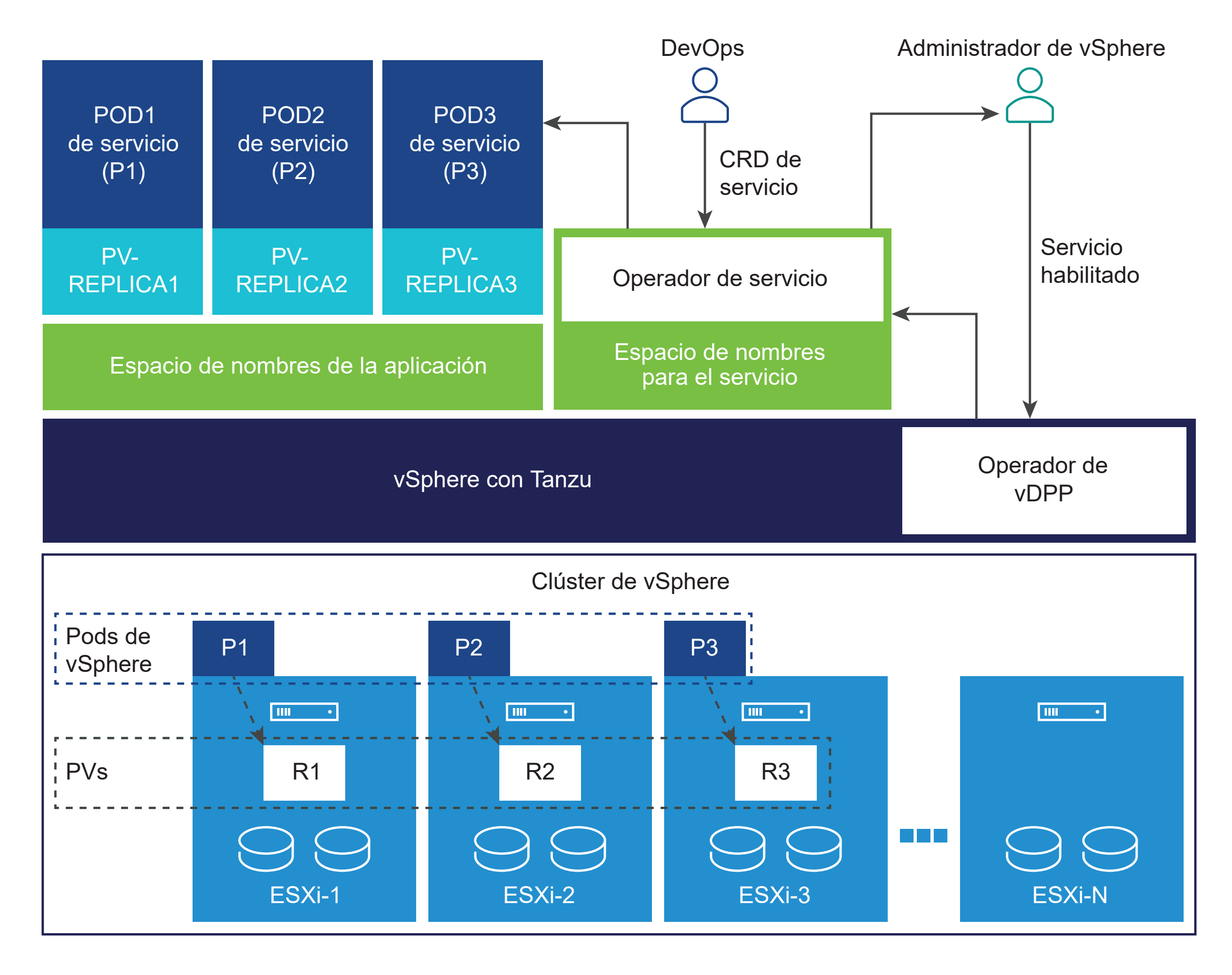
Siga estas recomendaciones generales a la hora de decidir qué tipo de vSAN debe utilizar.

- Utilice vSAN con SNA cuando quiera que la aplicación con estado nativa en la nube comparta la infraestructura física con otras máquinas virtuales comunes o con cargas de trabajo de Kubernetes. Cada carga de trabajo puede definir su propia directiva de almacenamiento y puede obtener lo mejor de ambos mundos desde un solo clúster.
- Use vSAN Direct, en cambio, si va a crear un clúster de hardware dedicado para los servicios nativos en la nube que no comparten nada.

Operador de la plataforma para la persistencia de datos de vSAN

El operador de la plataforma para la persistencia de datos de vSAN (vDPP, vSAN Data Persistence Platform) es un componente que se encarga de ejecutar y administrar los servicios con estado de partners integrados con vSphere. El operador de vDPP muestra los servicios con estado disponible al administrador de vSphere. Cuando el administrador de vSphere habilita un servicio persistente (por ejemplo, MinIO), el operador de vDPP implementa un operador específico de la aplicación para el servicio en el clúster supervisor.

Los operadores específicos de la aplicación son proporcionados por el tercero y deben ser compatibles con la vDPP. Por lo general, el operador ofrece un CRD que proporciona una interfaz de autoservicio con la que los usuarios de Kubernetes pueden crear instancias. vSphere with Tanzu usa este operador y el CRD para aprovisionar nuevas instancias de servicio, además de poder administrarlas y supervisarlas a través de la capa de servicios con estado. La mayoría de estos operadores utilizan conjuntos con estado para implementar sus instancias.



Una vez que el administrador de vSphere habilita un servicio, tiene lugar lo siguiente.

- El operador de vDPP activa un operador específico del servicio.
- El operador específico del servicio registra el complemento de la interfaz de usuario.
- Se crean directivas de almacenamiento optimizadas para el almacenamiento.

Límites de configuración para la plataforma de persistencia de datos de vSAN

VMware proporciona límites de configuración en la herramienta Valores máximos de configuración de VMware.

Valores máximos de persistencia de datos de vSAN	Límites
Cantidad máxima de volúmenes persistentes por plataforma de persistencia de datos de vSAN	1.000
Cantidad máxima de volúmenes persistentes por instancia de servicio en la plataforma de persistencia de datos de vSAN	De 60 a 80

Etiquetar dispositivos de almacenamiento para vSAN Direct

En las implementaciones de VMware Cloud Foundation, vSAN reclama automáticamente todos los dispositivos de almacenamiento local en su host ESXi. Puede hacer que los dispositivos no sean aptos para las instancias de vSAN habituales y estén disponibles para vSAN Direct.

En este tema se describe cómo se puede utilizar el comando `esxcli` para marcar los dispositivos como vSAN Direct. De forma alternativa, puede usar un script. Consulte Utilizar un script para etiquetar dispositivos de almacenamiento para vSAN Direct.

Procedimiento

1 Etiquete el dispositivo de almacenamiento local para vSAN Direct.

```
esxcli vsan storage tag add -d diskName -t vsanDirect
```

Por ejemplo:

```
esxcli vsan storage tag add -d mpx.vmhba0:C0:T1:L0 -t vsanDirect
```

El dispositivo dejará de ser apto para la instancia de vSAN regular.

2 Elimine la etiqueta vSAN Direct del dispositivo.

```
esxcli vsan storage tag remove -d diskName -t vsanDirect
```

Por ejemplo:

```
esxcli vsan storage tag remove -d mpx.vmhba0:C0:T1:L0 -t vsanDirect
```

Utilizar un script para etiquetar dispositivos de almacenamiento para vSAN Direct

En las implementaciones de VMware Cloud Foundation, puede usar un script para etiquetar los dispositivos HDD conectados a su host ESXi. Después de ejecutar el script, los dispositivos dejarán de ser aptos para la instancia de vSAN regular y estarán disponibles para vSAN Direct.

```
#!/usr/bin/env python3

# Copyright 2020 VMware, Inc. All rights reserved.

# Abstract
#
#    This script helps manage tagging of Direct Attached HDD disks
#    on ESXi systems for vSAN Direct in preparation for a VCF deployment.
#
#    It is expected to be used with ESX systems of version 7.0.1 or later.
```

```
#

import argparse
from enum import Enum
import logging
import sys
import os
import paramiko
import subprocess
import traceback
import ast
import getpass
from six.moves import input
from distutils.util import strtobool
from argparse import ArgumentParser

class ParseState(Enum):
        OPEN = 0
        DEVICE = 1

class RemoteOperationError(Exception):
    pass

class EsxVersion:

    def __init__(self, major, minor, release):
        self.major = major
        self.minor = minor
        self.release = release

    def __str__(self):
        return '{}.{}.{}'.format(self.major, self.minor, self.release)

    @staticmethod
    def build(str):
        tokens = str.split(b'.',3)
        return EsxVersion(int(tokens[0]), int(tokens[1]), int(tokens[2]))

class StorageDevice:

    def __init__(self, deviceId, isSSD, isVsanDirectEnabled):
        self.deviceId = str(deviceId.decode())
        self.isSSD = isSSD
        self.isVsanDirectCapable = True
        self.isVsanDirectEnabled = isVsanDirectEnabled

    def __str__(self):
        return '{}:\n\tIs SSD: {}\n\tvsanDirect enabled:{}'.format(
                    self.deviceId,
                    self.isSSD,
                    self.isVsanDirectEnabled)

    @staticmethod
    def strToBool(v):
        return bool(strtobool(str(v.decode())))
```

```
    @staticmethod
    def build(deviceId, props):
        vsanDirectEnabled = False
        isLocal = StorageDevice.strToBool(props[b'Is Local'])
        status = props[b'Status']
        isOffline = StorageDevice.strToBool(props[b'Is Offline'])
        isSSD = StorageDevice.strToBool(props[b'Is SSD'])
        isBootDevice = StorageDevice.strToBool(props[b'Is Boot Device'])
        deviceType = props[b'Device Type']
        if deviceType == b'Direct-Access' and isLocal and (not isOffline) and (not
isBootDevice) and status == b'on':
            return StorageDevice(deviceId, isSSD, vsanDirectEnabled)
        else:
            print("Skipping device {}".format(deviceId))
            return None

def parse_arguments():
    """
    Parses the command line arguments to the function
    """
    parser = argparse.ArgumentParser()
    parser.add_argument('--hostname', dest='hostname',
            help='specify hostname for the ESX Server', required=True)
    parser.add_argument('--username', dest='username',
            help='specify username to connect to the ESX Server', required=True)
    parser.add_argument('--password', dest='password',
            help='specify password to connect to the ESX Server', required=False)
    return parser.parse_args()

def get_esx_version(sshClient):
    global logger
    stdin_, stdout_, stderr_ = sshClient.exec_command('vmware -v')
    exit_status = stdout_.channel.recv_exit_status()
    if exit_status != 0:
        logger.error('Command exited with non-zero status: %s' % exit_status)
        logger.error('Error message: %s' % stderr_.read())
        raise RemoteOperationError('Failed to determine ESX version')
    output = stdout_.read()
    tokens = output.split()
    if len(tokens) < 3:
        raise RemoteOperationError('Invalid ESX Version - %s', output)
    return EsxVersion.build(tokens[2])

def check_esx_version(esxVersion):
    return esxVersion.major >= 7 and esxVersion.minor >= 0 and esxVersion.release >= 1

def query_devices(sshClient):
    global logger
    stdin_, stdout_, stderr_ = sshClient.exec_command('esxcli storage core device list')
    exit_status = stdout_.channel.recv_exit_status()
    if exit_status != 0:
        logger.error('Command exited with non-zero status: %s' % exit_status)
        logger.error('Error message: %s' % stderr_.read())
        raise RemoteOperationError('Failed to query core storage device list')
```

```
    output = stdout_.read()
    # Build the device list from the output
    return create_device_list(output)

def create_device_list(str):
    devices = []

    deviceId=""
    deviceProps={}

    parseState = ParseState.OPEN
    for line in str.splitlines():
        if parseState == ParseState.OPEN:
            if line.strip():
                deviceId=line.strip()
                parseState = ParseState.DEVICE
        elif parseState == ParseState.DEVICE:
            if line.strip():
                props = line.strip().split(b':',1)
                deviceProps[props[0]] = props[1].strip()
            else:
                if deviceId:
                    device = StorageDevice.build(deviceId, deviceProps)
                    if device:
                        devices.append(device)
                    else:
                        logger.debug("Skipping device {}".format(deviceId))
                deviceId=""
                deviceProps={}
                parseState = ParseState.OPEN
    if deviceId:
        device = StorageDevice.build(deviceId, deviceProps)
        if device:
            devices.append(device)
    return devices

def tag_device_for_vsan_direct(sshClient, deviceId):
    global logger
    logger.info("Tagging device [{}] for vSAN Direct".format(deviceId))
    command = "esxcli vsan storage tag add -d " + deviceId + " -t vsanDirect"
    stdin_, stdout_, stderr_ = sshClient.exec_command(command)
    exit_status = stdout_.channel.recv_exit_status()
    if exit_status != 0:
        logger.error('Command exited with non-zero status: %s' % exit_status)
        logger.error('Error message: %s' % stderr_.read())
        raise RemoteOperationError('Failed to tag device [{}] for vSAN
Direct'.format(deviceId))
    logger.info('Successfully tagged device [{}] for vSAN Direct'.format(deviceId))

def untag_device_for_vsan_direct(sshClient, deviceId):
    global logger
    logger.info("Untagging device [{}] for vSAN Direct".format(deviceId))
    command = "esxcli vsan storage tag remove -d " + deviceId + " -t vsanDirect"
    stdin_, stdout_, stderr_ = sshClient.exec_command(command)
    exit_status = stdout_.channel.recv_exit_status()
```

```
    if exit_status != 0:
        logger.error('Command exited with non-zero status: %s' % exit_status)
        logger.error('Error message: %s' % stderr_.read())
        raise RemoteOperationError('Failed to untag device [{}] for vSAN
Direct'.format(deviceId))
    logger.info('Successfully untagged device [{}] for vSAN Direct'.format(deviceId))

def get_vsan_info_for_device(sshClient, deviceId):
    global logger
    command = "vdq -q -d {}".format(deviceId)
    stdin_, stdout_, stderr_ = sshClient.exec_command(command)
    exit_status = stdout_.channel.recv_exit_status()
    if exit_status != 0:
        logger.error('Command exited with non-zero status: %s' % exit_status)
        logger.error('Error message: %s' % stderr_.read())
        raise RemoteOperationError('Failed to query vsan direct status on device [%s]' %
deviceId)
    output = stdout_.read()
    return ast.literal_eval(str(output.decode()))

def update_vsan_direct_status(sshClient, devices):
        for device in devices:
            vsanInfo = get_vsan_info_for_device(sshClient, device.deviceId)
            device.isVsanDirectEnabled = vsanInfo[0]['IsVsanDirectDisk'].strip() == "1"
            device.isVsanDirectCapable = vsanInfo[0]['State'].strip() == 'Eligible for use by
VSAN'

def getVsanDirectCapableDevices(devices):
    selectDevices = []
    # Cull devices incapable of vSAN Direct
    for device in devices:
        if device.isVsanDirectCapable:
            selectDevices.append(device)
    return selectDevices

def print_devices(devices):
    print("Direct-Attach Devices:")
    print("======================")
    iDevice = 0
    for device in devices:
        iDevice = iDevice + 1
        print ("{}. {}".format(iDevice, device))
    print("======================")

def tag_devices(sshClient, devices):
    for device in devices:
        tag_device_for_vsan_direct(sshClient, device.deviceId)

def untag_devices(sshClient, devices):
    for device in devices:
        untag_device_for_vsan_direct(sshClient, device.deviceId)

def tag_all_hdd_devices(sshClient, devices):
    hddDevices = []
    for device in devices:
```

```
        if not device.isSSD:
            hddDevices.append(device)
    if len(hddDevices) > 0:
        tag_devices(sshClient, hddDevices)

def show_usage():
    print ("==================================")
    print ("commands: {tag-all-hdd, tag, untag}")
    print ("\ttag <comma separated serial numbers of devices>")
    print ("\tuntag <comma separated serial numbers of devices>")
    print ("\ttag-all-hdd")
    print ("============")

def main():
    global logger
    logger.info('Tag disks for vSAN Direct')

    try:
        # Parse arguments
        args = parse_arguments()

        # 1. Setup SSH connection to ESX system
        sshClient = paramiko.SSHClient()
        sshClient.load_system_host_keys()
        sshClient.set_missing_host_key_policy(paramiko.AutoAddPolicy())
        passwd = args.password
        if passwd == None:
            passwd = getpass.getpass(prompt='Password: ')
        logger.info('Connecting to ESX System (IP: %s)' % args.hostname)
        sshClient.connect(args.hostname, username=args.username, password=passwd)
        # version check
        esxVersion = get_esx_version(sshClient)
        print('ESX Version on {} is {}'.format(args.hostname, esxVersion))
        logger.info('Checking ESX Version...')
        if not check_esx_version(esxVersion):
            raise Exception('ESX Version must be 7.0.1 or greater')

        print ('This script helps tag direct-attached disks for vSAN Direct on ESX')
        print ('Note: Only disks of type HDD are supported at this time.')
        print ()
        print ("For help, type help")
        show_usage()

        while True:
            # get device list
            print("Querying devices...")
            devices = query_devices(sshClient)
            # update devices with vSAN Direct status
            update_vsan_direct_status(sshClient, devices)
            # cull device list
            selectDevices = getVsanDirectCapableDevices(devices)
            # List the devices for the user to see
            print_devices(selectDevices)
            # find out what the user wants to do to these devices
            args = input('Command> ').split()
```

```
            if len(args) == 0:
                break
            cmd = args[0]
            if cmd == 'q' or cmd == 'quit' or cmd == 'exit':
                break
            elif cmd == 'help':
                show_usage()
            elif cmd == 'tag-all-hdd':
                print("Tagging all HDD devices...")
                tag_all_hdd_devices(sshClient, selectDevices)
            elif cmd == 'tag' or cmd == 'untag':
                chosenDevices = []
                if len(args) > 1:
                    serials = args[1].split(',')
                    for serialStr in serials:
                        serial = int(serialStr)
                        if serial < 1 or serial > len(selectDevices):
                            raise Exception("Error: Serial {} is out of range".format(serial))
                        chosenDevices.append(selectDevices[serial-1])
                if len(chosenDevices) == 0:
                    print("No devices specified")
                    continue
                if cmd == 'tag':
                    print("Tagging devices...")
                    tag_devices(sshClient, chosenDevices)
                else:
                    print("Untagging devices...")
                    untag_devices(sshClient, chosenDevices)
            else:
                print ("Error: Unrecognized command - %s" % cmd)
    except paramiko.ssh_exception.AuthenticationException as e:
        logger.error(e)
        sys.exit(5)
    except Exception as e:
        logger.error('Disk tagging failed with error: %s' % e)
        logger.error(traceback.format_exc())
        sys.exit(1)
    finally:
        # Close SSH client
        try:
            sshClient.close()
        except:
            pass

# Set up logging
logging.basicConfig()
logger = logging.getLogger('tag-disks-for-vsan-direct')

if __name__ == "__main__":
    main()
```

Configurar vSAN Direct para vSphere with Tanzu

Como administrador de vSphere, configure vSAN Direct para poder usarlo con la plataforma persistencia de datos de vSAN. Use dispositivos de almacenamiento sin reclamar que sean locales para el host ESXi.

Requisitos previos

Si vSAN reclama automáticamente todos los dispositivos de almacenamiento local de la implementación, use el comando `esxcli` para etiquetar los dispositivos que desea que estén disponibles para vSAN Direct. Consulte Etiquetar dispositivos de almacenamiento para vSAN Direct. De forma alternativa, puede usar un script. Para obtener información, consulte Utilizar un script para etiquetar dispositivos de almacenamiento para vSAN Direct.

Procedimiento

1 En vSphere Client, desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

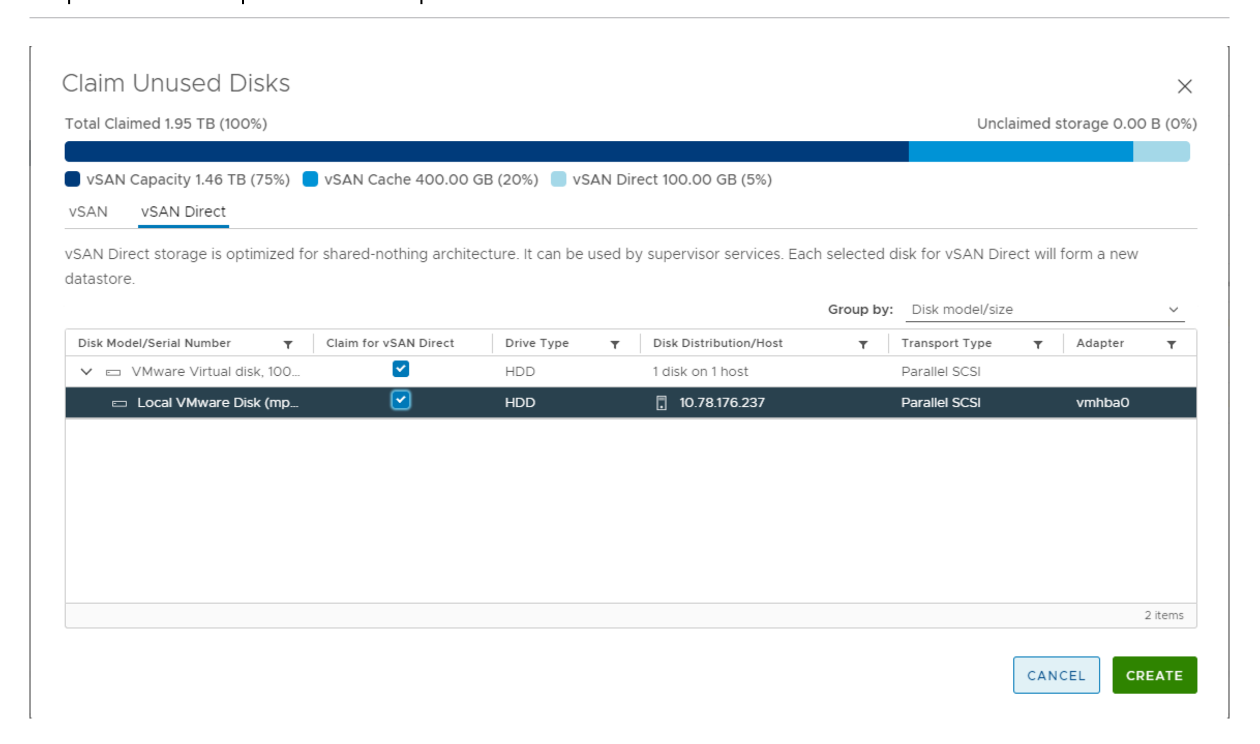
3 En vSAN, haga clic en **Administración de discos**.

4 Haga clic en **Reclamar discos sin utilizar**.

5 En el cuadro de diálogo **Reclamar discos sin utilizar**, haga clic en la pestaña **vSAN Direct**.

6 Seleccione un dispositivo para reclamar y seleccione una casilla de verificación en la columna **Reclamar para vSAN Direct** .

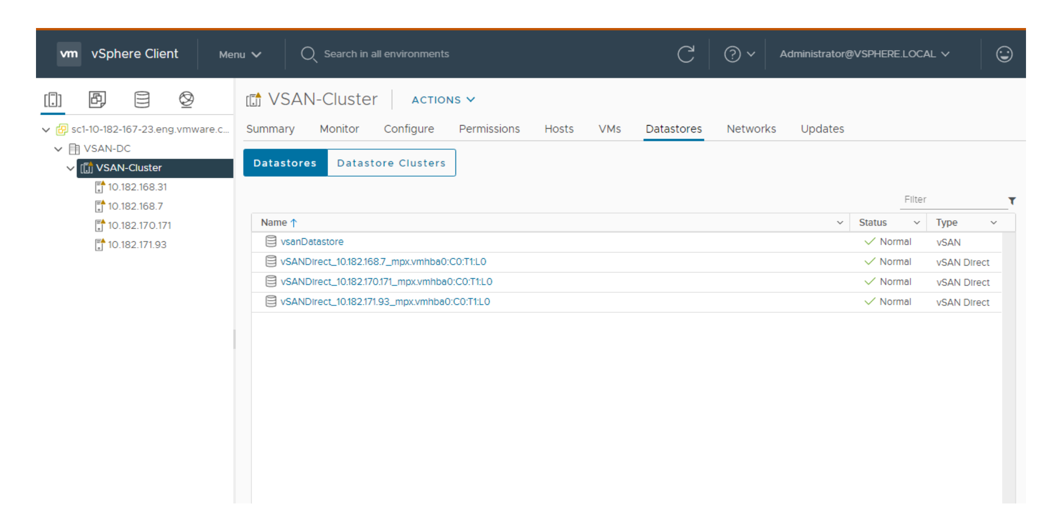
Nota Si reclamó los dispositivos para un almacén de datos de vSAN normal, estos dispositivos no aparecen en la pestaña **vSAN Direct** .



7 Haga clic en **Crear**.

En cada dispositivo que reclame, vSAN Direct crea un almacén de datos nuevo.

8 Haga clic en la pestaña **Almacenes de datos** para mostrar todos los almacenes de datos de vSAN Direct en el clúster.



Pasos siguientes

Puede utilizar vSAN Direct con almacenamiento externo. Para obtener más información, consulte Usar almacenamiento externo con vSAN Direct.

Habilitar servicios con estado en vSphere with Tanzu

vSphere with Tanzu se integra con varios servicios de terceros que utilizan la plataforma de persistencia de datos de vSAN para satisfacer sus necesidades de almacenamiento persistente. Como administrador de vSphere, habilite los servicios en vCenter Server.

A partir de la versión vSphere with Tanzu 7.0 Update 3, puede descargar los servicios de terceros que estén disponibles desde un repositorio compatible con VMware.

Cuando habilite el servicio con estado, primero debe registrar el servicio con vCenter Server mediante el archivo YAML descargado que describe el servicio. Después, instale el servicio en los clústeres supervisor para que los ingenieros de desarrollo y operaciones puedan utilizar el servicio en las cargas de trabajo de Kubernetes.

Requisitos previos

- Privilegio necesario: **Servicios de supervisor.Administrar servicios de supervisor**
- Asegúrese de que el clúster supervisor utilice la pila de redes de NSX-T Data Center. La plataforma persistencia de datos de vSAN no admite redes de vSphere Distributed Switch (vDS).

  Para obtener información sobre cómo configurar NSX-T, consulte Configurar NSX-T Data Center para vSphere with Tanzu.

- Descargue un archivo YAML del servicio de partners desde el repositorio que mantiene VMware.

  Cuando descargue los archivos YAML del servicio, asegúrese de utilizar la versión del servicio correcta que es compatible con su versión de vSphere.

  Si instaló versiones anteriores de los servicios de partners, MinIO y Cloudian Hyperstore, actualícelas a las versiones compatibles después de actualizar vSphere a la versión 7.0 Update 3. Las versiones más recientes de los operadores de partners solucionan ciertos problemas y utilizan nuevas funciones de la plataforma. Para obtener más información, consulte la documentación del partner.

  Tabla 10-1. Matriz de compatibilidad para vSphere y los servicios de partners

Versión de vSphere	Servicio de partners	Versión del servicio	Versión de Kubernetes
vSphere 7.0 Update 3	MinIO	2.0.0	1.19, 1.20, 1.21
	Cloudian	1.2.0	1.19, 1.20, 1.21

  Utilice uno de los siguientes métodos para descargar el archivo YAML:

  - En el repositorio de https://vmwaresaas.jfrog.io/, vaya a una carpeta de partner adecuada en **Artefactos > vDPP-Partner-YAML** y seleccione un archivo YAML para descargarlo.

    La versión más reciente del archivo YAML de partner se encuentra en el directorio de partners de nivel superior.

  - Utilice los comandos `wget` o `curl` para descargar los archivos YAML.

    Por ejemplo:

    ```
    wget https://vmwaresaas.jfrog.io/artifactory/vDPP-Partner-YAML/Cloudian/Hyperstore/
    SupervisorService/hyperstore-supervisorservice.yaml
    ```

Procedimiento

1 Configure el almacenamiento de vSAN o vSAN Direct.

  Para obtener información sobre cómo configurar el almacenamiento de vSAN, consulte la *Administrar VMware vSAN*. Para configurar vSAN Direct, consulte Configurar vSAN Direct para vSphere with Tanzu.

  Los almacenes de datos de vSAN Direct aparecen en Kubernetes como StoragePools.

2 Agregue un servicio con estado al sistema de vCenter Server.

  Utilice el archivo YAML del servicio de partners que descargó del repositorio que mantiene VMware.

  Consulte Agregar una instancia de servicio de supervisor a vCenter Server.

3 Instale el servicio en los clústeres supervisor.

  Consulte Instalar un servicio de supervisor en clústeres supervisor.

Después de habilitar el servicio, la plataforma persistencia de datos de vSAN realiza las siguientes acciones para crear los recursos necesarios para el servicio:

- Crea un espacio de nombres para este servicio en el clúster de supervisor.
- Crea directivas de almacenamiento predeterminadas y las clases de almacenamiento correspondientes que se utilizarán con almacenes de datos vSAN SNA (Shared-Nothing-Architecture) y vSAN Direct.

  Nota La plataforma persistencia de datos de vSAN crea automáticamente las clases de almacenamiento vsan-direct y vsan-sna en el espacio de nombres después de que un administrador de vSphere habilite el servicio con estado. Solo las aplicaciones que se ejecutan en el clúster supervisor pueden utilizar las clases de almacenamiento vsan-direct y vsan-sna. Estas clases de almacenamiento no se pueden utilizar dentro de un clúster de Tanzu Kubernetes.

  En vSphere 7.0 Update 2 y otras versiones posteriores, la directiva de almacenamiento vSAN Direct se basa en las capacidades. Si creó directivas basadas en etiquetas en vSphere 7.0 Update 1, estas se convierten automáticamente en directivas basadas en capacidades después de actualizar a vSphere 7.0 Update 2 y otras versiones posteriores.

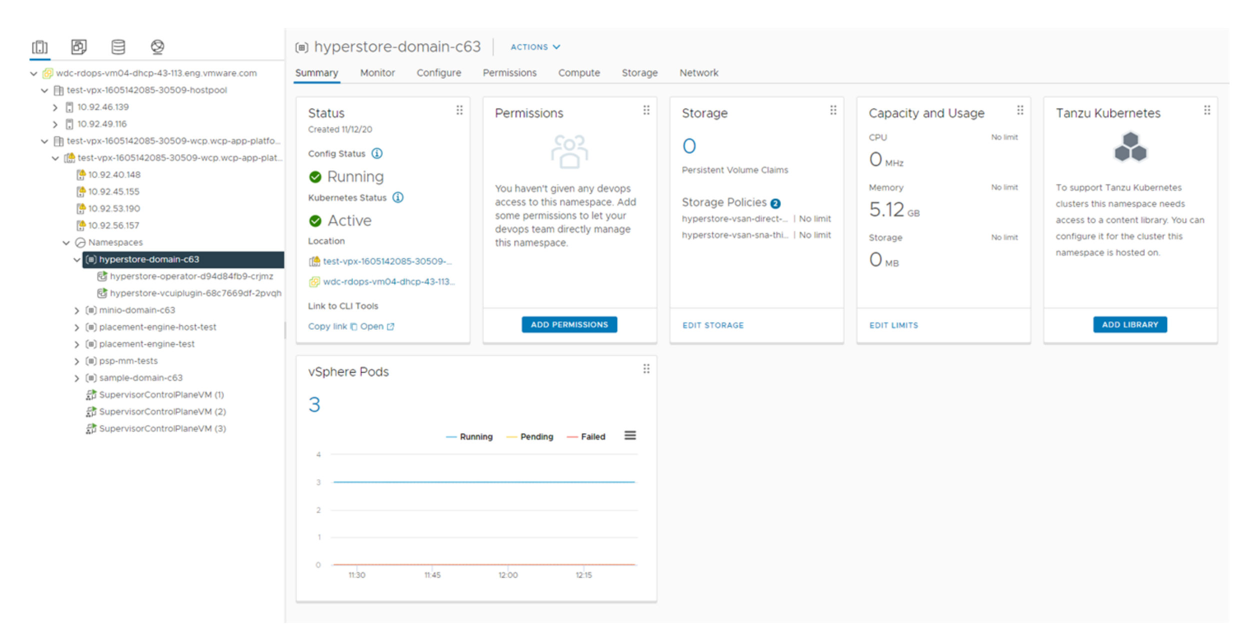
  Si desea crear nuevas directivas de almacenamiento y asignarlas al espacio de nombres del servicio en lugar de usar las predeterminadas, consulte Crear directiva de almacenamiento de vSAN Direct y Crear directiva de almacenamiento SNA vSAN.

- Crea funciones de desarrollo y operaciones, incluidas las funciones con permisos de edición y visualización.

  Cuando se implementa el operador de servicio, sus objetos CRD personalizados se instalan en el clúster supervisor. Los usuarios con permiso de edición pueden tener recursos CRUD de estas definiciones de recursos personalizados (Custom Resource Definitions, CRD) en el espacio de nombres. Los usuarios con permiso de vista solo pueden ver los recursos de esta CRD.

- Si el tercero proporcionó un complemento de interfaz de usuario personalizado, este aparecerá en vSphere Client. El administrador de vSphere puede utilizar el complemento para administrar el servicio.

4 Seleccione el espacio de nombres que se ha creado para el servicio y haga clic en la pestaña **Resumen** para verificar que se hayan creado todos los recursos apropiados para el servicio.



Pasos siguientes

- El ingeniero de desarrollo y operaciones utiliza el comando `kubectl` para acceder al espacio de nombres del servicio y utiliza los CRD de terceros para implementar instancias del servicio de aplicaciones de terceros. Si desea obtener más información, consulte la documentación de terceros.

  Para comprobar que el espacio de nombres que utiliza para los servicios con estado tiene las clases de almacenamiento adecuadas, consulte Comprobar las directivas de almacenamiento disponibles para los servicios con estado.

- Si el tercero proporcionó un complemento de interfaz de usuario personalizado, el administrador de vSphere puede utilizar el complemento para administrar y supervisar el servicio.

  Para obtener más información, consulte la documentación del complemento de interfaz de usuario de tercero. Además, el administrador de vSphere puede utilizar las comprobaciones de Skyline Health para supervisar los servicios. Consulte Supervisar servicios con estado en vSphere with Tanzu.

Supervisar servicios con estado en vSphere with Tanzu

Después de habilitar los servicios con estado integrados de terceros, utilice las funciones de supervisión de capacidad y estado de vSAN para ver el estado y analizar el uso que hacen del espacio los objetos de servicio.

Procedimiento

1 En vSphere Client, desplácese hasta clúster supervisor.

2 Haga clic en la pestaña **Supervisar**.

3 Supervise los objetos virtuales que se ejecutan en el espacio de nombres que corresponde al servicio habilitado.

   a En **vSAN**, haga clic en **Objetos virtuales**.

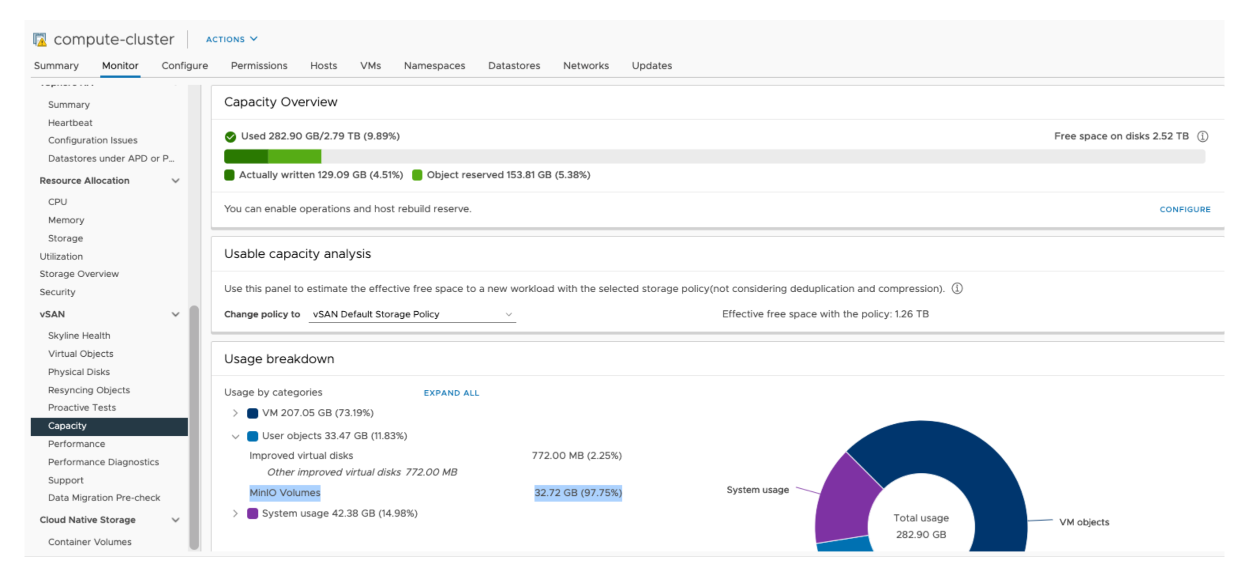
      Puede examinar los objetos virtuales, como los objetos del operador de MinIO, y comprobar su estado.

   b Para ver la colocación del objeto en toda la infraestructura física, seleccione un objeto concreto y haga clic en **VER DETALLES DE COLOCACIÓN**.

4 Supervise la capacidad que utilizan los objetos de servicio.

   a En **vSAN**, haga clic en **Capacidad**.

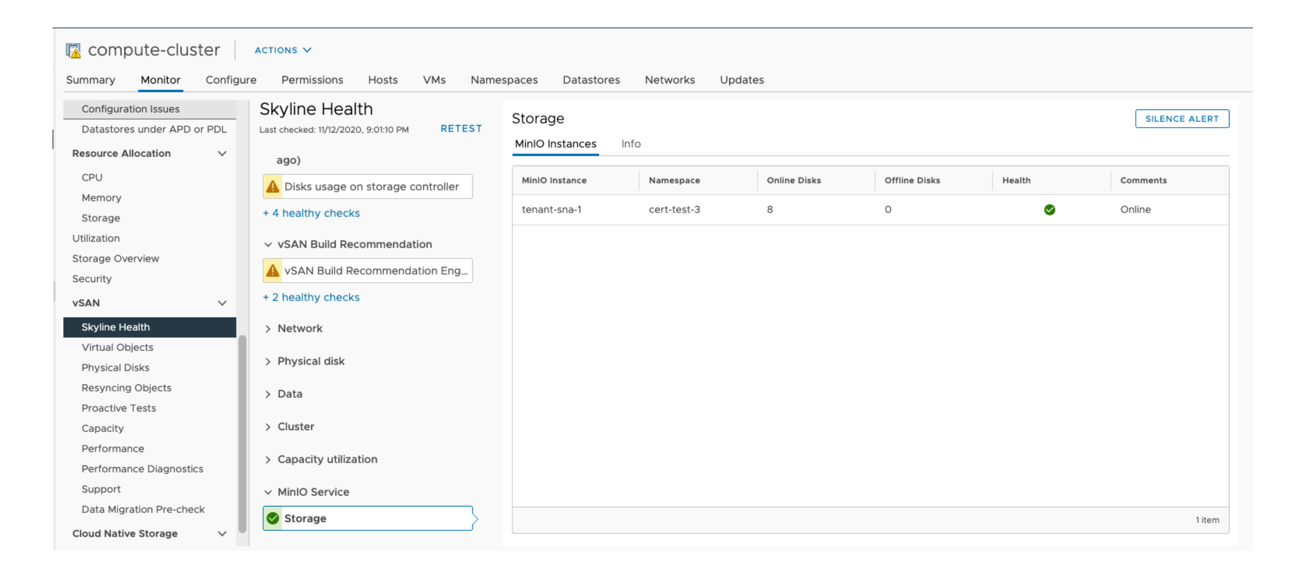
   b En el panel **Desglose de uso**, muestre los objetos de servicio en **Objetos de usuario**.



5 Supervise el estado de las instancias del servicio.

   a En **vSAN**, seleccione **Skyline Health**.

   b Seleccione una comprobación de estado de servicio individual para ver la información detallada.



Comprobar las directivas de almacenamiento disponibles para los servicios con estado

Como ingeniero de desarrollo y operaciones, compruebe que el espacio de nombres que utiliza para los servicios con estado en el entorno vSphere with Tanzu tenga las clases de almacenamiento adecuadas. Las clases de almacenamiento pueden ser Shared-Nothing-Architecture (SNA) de vSAN y vSAN Direct.

La plataforma persistencia de datos de vSAN crea automáticamente estas clases de almacenamiento en el espacio de nombres después de que un administrador de vSphere habilite el servicio con estado. Consulte Habilitar servicios con estado en vSphere with Tanzu.

Nota Solo las aplicaciones que se ejecutan en el clúster supervisor pueden utilizar las clases de almacenamiento vsan-direct y vsan-sna. Estas clases de almacenamiento no se pueden utilizar dentro de un clúster de Tanzu Kubernetes.

Además de las clases de almacenamiento predeterminadas, el administrador de vSphere también puede crear directivas de almacenamiento personalizadas y asignarlas al espacio de nombres. Consulte Crear directiva de almacenamiento de vSAN Direct y Crear directiva de almacenamiento SNA vSAN.

Procedimiento

- Compruebe que las directivas de almacenamiento que se usarán con vSAN SNA y vSAN Direct estén disponibles en el espacio de nombres.



```
# kubectl get sc
NAME                         PROVISIONER              RECLAIMPOLICY   VOLUMEBINDINGMODE
ALLOWVOLUMEEXPANSION   AGE
sample-vsan-direct-thick   csi.vsphere.vmware.com   Delete          WaitForFirstConsumer
```

```
true                    3m36s
sample-vsan-sna-thick       csi.vsphere.vmware.com   Delete          WaitForFirstConsumer
true                    13m
```

Crear directiva de almacenamiento SNA vSAN

Si utiliza vSAN con una plataforma persistencia de datos de vSAN, puede crear una directiva de almacenamiento de arquitectura de no compartir nada (SNA) vSAN para usarla con el espacio de nombres donde se ejecutan los servicios con estado.

Procedimiento

1 En vSphere Client, abra el asistente **Crear directiva de almacenamiento de máquina virtual**.

   a En el menú **Inicio**, haga clic en **Directivas y perfiles**.

   b En **Directivas y perfiles**, haga clic en **Directivas de almacenamiento de máquina virtual**.

   c Haga clic en **Crear**.

2 Introduzca el nombre y la descripción de la directiva.

Opción	Acción
vCenter Server	Seleccione la instancia de vCenter Server.
Nombre	Introduzca el nombre de la directiva de almacenamiento, por ejemplo, **`Ejemplo de SNA grueso`**.
Descripción	Introduzca la descripción de la directiva de almacenamiento.

3 En la página **Estructura de directiva**, en **Reglas específicas de almacenes de datos**, habilite las reglas para la colocación del almacenamiento de vSAN.

4 En la página **vSAN**, haga clic en la pestaña **Disponibilidad** y seleccione los siguientes valores. Los valores solo se aplican a las cargas de trabajo de SNA en la plataforma persistencia de datos de vSAN. No se pueden utilizar para aprovisionar cargas de trabajo de máquinas virtuales.

Opción	Descripción
Opción	Valor
Tolerancia de desastres en el sitio	**Ninguno: clúster estándar** **Nota** La plataforma persistencia de datos de vSAN solo admite clústeres estándares.
Errores que se toleran	**No hay redundancia de datos con afinidad de host**

Aprovisionamiento grueso aplicado para las cargas de trabajo de SNA y se selecciona como un valor para la reserva de espacio de objetos en la pestaña **Reglas de directivas avanzadas**. No puede cambiar este valor.

5 En la página **Compatibilidad de almacenamiento**, revise la lista de almacenes de datos de vSAN que coinciden con esta directiva.

6 En la página **Revisar y finalizar**, revise la configuración de la directiva de almacenamiento y haga clic en **Finalizar**.

   Para cambiar una configuración, haga clic en **Atrás** para volver a la página correspondiente.

Pasos siguientes

Después de crear la directiva, puede asignarla al espacio de nombres donde se ejecuta el servicio con estado. Consulte Cambiar la configuración de almacenamiento en un espacio de nombres.

Crear directiva de almacenamiento de vSAN Direct

Si utiliza vSAN Direct con la plataforma persistencia de datos de vSAN, puede crear una directiva de almacenamiento basada en capacidades que se utilizará con el espacio de nombres donde se ejecutan los servicios con estado.

Procedimiento

1 En vSphere Client, abra el asistente **Crear directiva de almacenamiento de máquina virtual**.

   a En el menú **Inicio**, haga clic en **Directivas y perfiles**.

   b En **Directivas y perfiles**, haga clic en **Directivas de almacenamiento de máquina virtual**.

   c Haga clic en **Crear**.

2 Introduzca el nombre y la descripción de la directiva.

Opción	Acción
vCenter Server	Seleccione la instancia de vCenter Server.
Nombre	Introduzca el nombre de la directiva de almacenamiento, por ejemplo, `Ejemplo de vSAN Direct grueso`.
Descripción	Introduzca la descripción de la directiva de almacenamiento.

3 En la página **Estructura de directiva**, en **Reglas específicas de almacenes de datos**, habilite las reglas para la colocación del almacenamiento de vSAN Direct.

4 En la página **Reglas de vSAN Direct**, especifique vSAN Direct como un tipo de colocación de almacenamiento.

5 En la página **Compatibilidad de almacenamiento**, revise la lista de almacenes de datos de vSAN Direct que coinciden con esta directiva.

6 En la página **Revisar y finalizar**, revise la configuración de la directiva de almacenamiento y haga clic en **Finalizar**.

   Para cambiar una configuración, haga clic en **Atrás** para volver a la página correspondiente.

Pasos siguientes

Después de crear la directiva, puede asignarla al espacio de nombres donde se ejecuta el servicio con estado. Consulte Cambiar la configuración de almacenamiento en un espacio de nombres.

Implementar cargas de trabajo en pods de vSphere

11

Como ingeniero de desarrollo y operaciones, puede implementar y administrar el ciclo de vida de los pods de vSphere dentro de los límites de recursos de un espacio de nombres que se ejecuta en un clúster supervisor. Debe tener permisos de escritura en un espacio de nombres para implementar los pods de vSphere en él.

Este capítulo incluye los siguientes temas:

- Obtener y utilizar el contexto del clúster supervisor
- Implementar una aplicación en un pod de vSphere en un espacio de nombres de vSphere
- Implementar una aplicación en un pod de vSphere mediante el registro de Harbor integrado
- Ampliar una aplicación de pod de vSphere
- Implementar un pod de vSphere confidencial

Obtener y utilizar el contexto del clúster supervisor

Después de que el administrador de vSphere le proporcione la dirección IP del plano de control de Kubernetes en clúster supervisor, puede iniciar sesión en clúster supervisor y obtener los contextos a los que tiene acceso. Los contextos corresponden a los espacios de nombres de clúster supervisor.

Requisitos previos

- Obtenga de su administrador de vSphere la dirección IP del plano de control de Kubernetes de clúster supervisor.
- Obtenga su cuenta de usuario en vCenter Single Sign-On.
- Compruebe con el administrador de vSphere si tiene permisos para acceder a los contextos que necesita.
- Para comprobar que el certificado ofrecido por el plano de control de Kubernetes sea de confianza en el sistema, instale la CA de firma como raíz de confianza o agregue el certificado directamente como raíz de confianza.

Procedimiento

1 En una ventana del explorador, abra la dirección URL del plano de control de Kubernetes.

2 Compruebe de que la suma de comprobación SHA256 de `vsphere-plugin.zip` coincida con la suma de comprobación del archivo `sha256sum.txt`.

3 Descargue el archivo `vsphere-plugin.zip` en su máquina y establézcalo en la ruta de búsqueda de archivos ejecutables del sistema operativo.

4 En una ventana del símbolo del sistema, ejecute el siguiente comando para iniciar sesión en vCenter Server:

```
kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user
account name>
```

5 Para ver los detalles de los contextos de configuración a los que puede acceder, ejecute el siguiente comando de `kubectl`:

```
kubectl config get-contexts
```

La CLI muestra los detalles de cada contexto disponible.

6 Para cambiar de contexto, utilice el siguiente comando:

```
kubectl config use-context <example-context-name>
```

Resultados

Se invoca la API de inicio de sesión en el plano de control de Kubernetes. Un proxy de autenticación redirecciona una solicitud de autenticación a vCenter Single Sign-On. vCenter Server devuelve un token web JSON y lo agrega al archivo `kubeconfig`. Ese token se envía al plano de control de Kubernetes con cada nuevo comando kubectl para autenticar al usuario.

Implementar una aplicación en un pod de vSphere en un espacio de nombres de vSphere

Puede implementar una aplicación en un espacio de nombres en un clúster supervisor. Una vez que se implementa la aplicación, se crea la cantidad correspondiente de instancias de pods de vSphere en el clúster supervisor del espacio de nombres.

También puede implementar aplicaciones a partir de imágenes almacenadas en el registro de la imagen de Harbor. Consulte Implementar una aplicación en un pod de vSphere mediante el registro de Harbor integrado.

Requisitos previos

- Obtenga de su administrador de vSphere la dirección IP del plano de control de Kubernetes de clúster supervisor.
- Obtenga su cuenta de usuario en vCenter Single Sign-On.
- Compruebe con el administrador de vSphere si tiene permisos para acceder a los contextos que necesita.

Procedimiento

1 Realice la autenticación con clúster supervisor.

Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

2 Cambie al contexto en el que desea implementar la aplicación.

```
kubectl config use-context <namespace>
```

3 Implemente la aplicación.

```
kubectl apply -f <application name>.yaml
```

Implementar una aplicación en un pod de vSphere mediante el registro de Harbor integrado

Puede utilizar imágenes almacenadas en el registro de Harbor para implementar pods de vSphere en los espacios de nombres del clúster supervisor.

Requisitos previos

- Inserte imágenes en un proyecto en registro de Harbor que tenga el mismo nombre que el espacio de nombres en el que desea implementar la aplicación. Consulte Insertar imágenes en el registro de Harbor integrado .
- Agregue el contenido de `vspere-plugin.zip` a la ruta de acceso del archivo de ejecución de su entorno.

Procedimiento

1 Cree un archivo YAML que contenga los siguientes parámetros:

```
...
namespace: <namespace-name>
...
spec:
...
image: <image registry URL>/<namespace name>/<image name>
```

2 Inicie sesión en el clúster supervisor:

```
kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user
account name>
```

3 Cambie al espacio de nombres en el que desea implementar la aplicación.

```
kubectl config use-context <namespace>
```

4 Implemente una pod de vSphere desde ese archivo YAML:

```
kubectl apply -f <yaml file name>.yaml
```

5 Ejecute el siguiente comando para comprobar que la imagen se extrae de registro de Harbor y que la pod de vSphere está en estado de ejecución:

```
kubectl describe pod/<yaml name>
```

Resultados

El archivo YAML que creó se implementa en el espacio de nombres especificado mediante la imagen del proyecto en registro de Harbor que recibe el nombre del espacio de nombres.

Ejemplo:

Cree e implemente el siguiente archivo de YAML en el espacio de nombres demoapp1 mediante la imagen de BusyBox del proyecto de demoapp1 en registro de Harbor:

```
apiVersion: v1
kind: Pod
metadata:
  name: busybox
  namespace: demoapp1
spec:
  containers:
  - name: busybox
    image: <harbor_IP>/demoapp1/busybox:latest
    command:
      - sleep
      - "3600"
    imagePullPolicy: IfNotPresent
  restartPolicy: Always
```

Ampliar una aplicación de pod de vSphere

Puede realizar un escalado o reducción verticales de la cantidad de réplicas para cada aplicación que se ejecute en un clúster supervisor.

Requisitos previos

- Obtenga de su administrador de vSphere la dirección IP del plano de control de Kubernetes de clúster supervisor.
- Obtenga su cuenta de usuario en vCenter Single Sign-On.
- Compruebe con el administrador de vSphere si tiene permisos para acceder a los contextos que necesita.

Procedimiento

1 Realice la autenticación con clúster supervisor.

```
kubectl vsphere login --server <control plane load balancer IP address> --vsphere-username
<vSphere user account name>
```

2 Escalado o reducción verticales de una aplicación.

```
kubectl get deployments
kubectl scale deployment <deployment-name> --replicas=<number-of-replicas>
```

Implementar un pod de vSphere confidencial

Con vSphere with Tanzu, puede ejecutar pods de vSphere confidenciales en un clúster supervisor. Un pod de vSphere confidencial utiliza una tecnología de hardware que mantiene cifrada la memoria del sistema operativo invitado, lo que la protege del acceso desde el hipervisor.

A partir de vSphere 7.0 Update 2, puede crear pods de vSphere confidenciales. Para ello, agregue el estado cifrado de SEV (Secure Encrypted Virtualization-Encrypted State, SEV-ES) como una mejora de seguridad adicional. SEV-ES impide que los registros de la CPU filtren información en los registros de los componentes como el hipervisor. SEV-ES también puede detectar modificaciones malintencionadas en un estado de registro de la CPU. Para obtener más información sobre el uso de la tecnología SEV-ES en el entorno de vSphere, consulte Proteger máquinas virtuales con virtualización cifrada segura de AMD: estado cifrado.

Requisitos previos

Para habilitar SEV-ES en un host ESXi, el administrador de vSphere debe seguir estas directrices:

- Utilice los hosts que admiten la funcionalidad SEV-ES. Actualmente, SEV-ES solo es compatible con las CPU AMD EPYC 7xx2 (cuyo nombre de código es *Rome*) y CPU posteriores.
- Utilice ESXi versión 7.0 Update 2 o posteriores.
- Habilite SEV-ES en la configuración de la BIOS del sistema de un ESXi. Consulte la documentación del sistema para obtener más información sobre cómo acceder a la configuración de la BIOS.
- Al hacerlo, introduzca un valor para la opción de **ASID mínimo de estado no cifrado de SEV** que sea igual a la cantidad de máquinas virtuales de SEV-ES y pods de vSphere confidenciales en el host más una. Por ejemplo, si tiene pensado ejecutar 100 máquinas virtuales de SEV-ES y 128 pods de vSphere, introduzca al menos 229. Puede introducir una configuración de hasta 500.

Procedimiento

1 Cree un archivo YAML que contenga los siguientes parámetros.

a En las anotaciones, habilite la función de pods de vSphere confidencial.

```
...
annotations:
        vmware/confidential-pod: enabled
...
```

b Especifique los recursos de memoria para los contenedores.

Asegúrese de establecer las solicitudes de memoria y los límites de memoria en el mismo valor que en este ejemplo.

```
resources:
      requests:
        memory: "512Mi"
      limits:
        memory: "512Mi"
```

Utilice el siguiente archivo YAML como ejemplo:

```
apiVersion: v1
kind: Pod
metadata:
  name: photon-pod
  namespace: my-podvm-ns
  annotations:
    vmware/confidential-pod: enabled
spec:  # specification of the pod's contents
  restartPolicy: Never
  containers:
  - name: photon
    image: wcp-docker-ci.artifactory.eng.vmware.com/vmware/photon:1.0
    command: ["/bin/sh"]
    args:    ["-c", "while true; do echo hello, world!; sleep 1; done"]
    resources:
      requests:
        memory: "512Mi"
      limits:
        memory: "512Mi"
```

2 Inicie sesión en clúster supervisor.

```
kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user
account name>
```

3 Cambie al espacio de nombres en el que desea implementar la aplicación.

```
kubectl config use-context <namespace>
```

4 Implemente un pod de vSphere confidencial desde el archivo YAML.

```
kubectl apply -f <yaml file name>.yaml
```

Nota Cuando se implementa el pod de vSphere, DRS lo coloca en el nodo ESXi compatible con SEV-ES. Si no hay ningún nodo disponible, el pod de vSphere se marca como con errores.

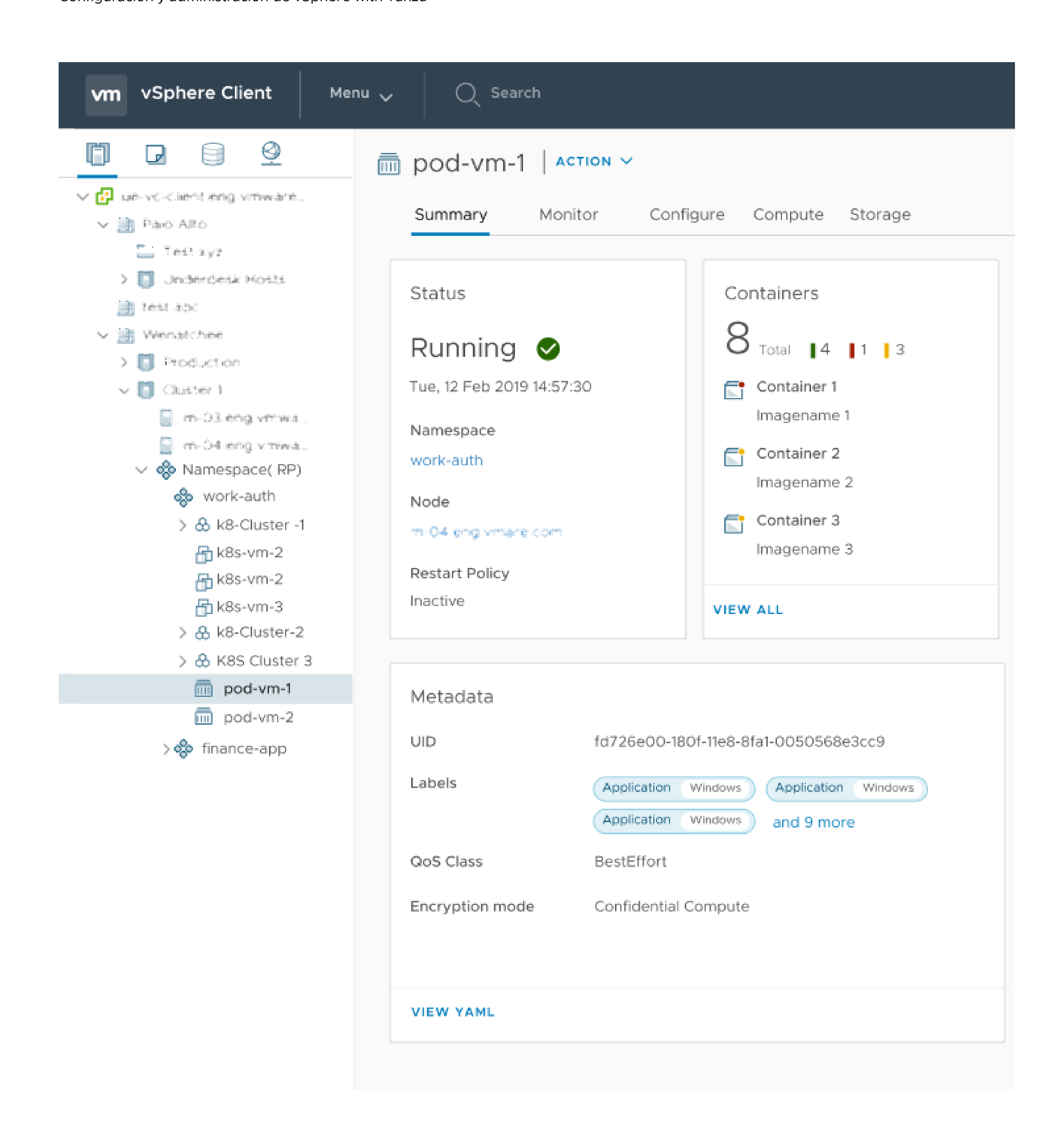
El pod de vSphere confidencial que se inicia proporciona compatibilidad con el cifrado de memoria de hardware para todas las cargas de trabajo que se ejecutan en ese pod.

5 Ejecute el siguiente comando para comprobar que se creó el pod de vSphere confidencial.

```
kubectl describe pod/<yaml name>
```

Pasos siguientes

Un administrador de vSphere puede ver el pod de vSphere confidencial. En el vSphere Client, aparece con la etiqueta **Modo de cifrado: Cálculo confidencial**.



vm vSphere Client
Menu
Search
pod-vm-1
ACTION
Summary
Monitor
Configure
Compute
Storage
Namespace(RP)
work-auth
k8-Cluster -1
k8s-vm-2
k8s-vm-2
k8s-vm-3
k8-Cluster-2
K8S Cluster 3
pod-vm-1
pod-vm-2
finance-app
Status
Running
Tue, 12 Feb 2019 14:57:30
Namespace
work-auth
Node
Restart Policy
Inactive
Containers
8 Total 4 1 3
Container 1
Imagename 1
Container 2
Imagename 2
Container 3
Imagename 3
VIEW ALL
Metadata
UID
fd726e00-180f-11e8-8fa1-0050568e3cc9
Labels
Application Windows
Application Windows
Application Windows
and 9 more
QoS Class
BestEffort
Encryption mode
Confidential Compute
VIEW YAML

Implementar y administrar máquinas virtuales en vSphere with Tanzu

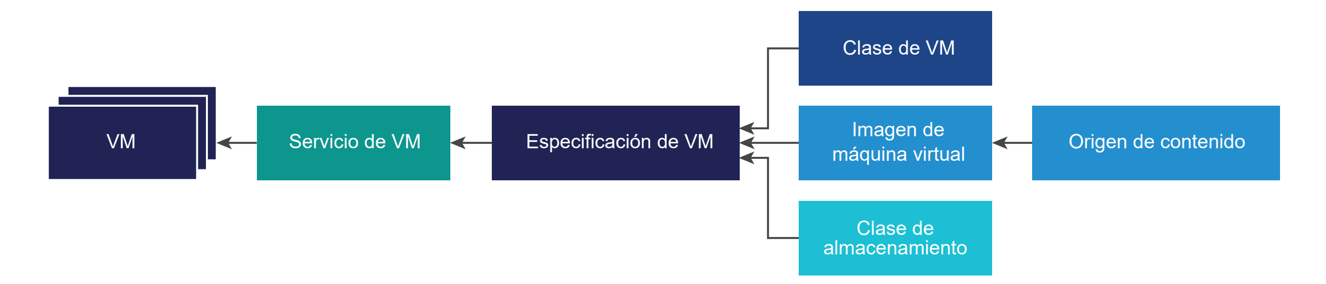
12

vSphere with Tanzu ofrece una funcionalidad de servicio de máquina virtual que permite a los ingenieros de desarrollo y operaciones implementar y ejecutar máquinas virtuales, además de contenedores, en un entorno de Kubernetes común y compartido. Puede utilizar el servicio de máquina virtual para administrar el ciclo de vida de las máquinas virtuales en un espacio de nombres de vSphere. El servicio de máquina virtual administra las máquinas virtuales independientes y las máquinas virtuales que conforman los clústeres de Tanzu Kubernetes.

Por lo general, sus necesidades y objetivos comerciales influyen en la decisión de ejecutar cargas de trabajo en una máquina virtual en lugar de en un contenedor. Para obtener información sobre cuándo ejecutar una máquina virtual, consulte Usar máquinas virtuales en vSphere with Tanzu.

Conceptos del servicio de máquina virtual

Para describir el estado de una máquina virtual que se implementará en un espacio de nombres de vSphere, utilice parámetros como una clase de máquina virtual, una imagen de máquina virtual y una clase de almacenamiento. A continuación, el servicio de máquina virtual reúne estas especificaciones para crear máquinas virtuales independientes o máquinas virtuales que admitan clústeres de Tanzu Kubernetes.



Servicio de VM

El servicio de máquina virtual es un componente de vSphere with Tanzu que proporciona una API declarativa de tipo Kubernetes para la administración de las máquinas virtuales y los recursos de vSphere asociados. El servicio de máquina virtual permite a los administradores de vSphere entregar recursos y proporcionar plantillas, como clases e imágenes de máquinas virtuales, a Kubernetes. Los ingenieros de desarrollo y operaciones pueden utilizar estos

recursos para describir el estado deseado de una máquina virtual. Después de que los ingenieros de desarrollo y operaciones especifiquen el estado de la máquina virtual, el servicio de máquina virtual convierte el estado deseado en un estado realizado en función de los recursos de la infraestructura de respaldo.

Una máquina virtual creada a través del servicio de máquina virtual solo se puede administrar desde el espacio de nombres de Kubernetes con los comandos de `kubectl`. Los administradores de vSphere no pueden administrar la máquina virtual desde vSphere Client, pero pueden mostrar sus detalles y supervisar los recursos que utiliza. Para obtener información, consulte Supervisar máquinas virtuales disponibles en vSphere with Tanzu.

Clase de VM

La clase de máquina virtual es una especificación de máquina virtual que se puede utilizar para solicitar un conjunto de recursos para una máquina virtual. La clase de máquina virtual es controlada y administrada por un administrador de vSphere, y define parámetros como el número de CPU virtuales, la capacidad de memoria y la configuración de reserva. Los parámetros definidos están avalados y garantizados por los recursos de infraestructura subyacentes de un clúster supervisor.

Un administrador de vSphere puede crear clases de máquinas virtuales personalizadas.

Además, la administración de cargas de trabajo ofrece varias clases de máquinas virtuales predeterminadas. Por lo general, cada tipo de clase predeterminada viene en dos ediciones: garantizada y de mejor esfuerzo. Una edición garantizada reserva por completo los recursos que solicita una especificación de máquina virtual. Una edición de clase de mejor esfuerzo no lo hace, y permite que los recursos se sobreasignen. Por lo general, en un entorno de producción, se utiliza un tipo garantizado.

A continuación, se muestran ejemplos de clases de máquinas virtuales predeterminadas.

Clase	CPU	Memoria (GB)	CPU y memoria reservadas
`guaranteed-large`	4	16	Sí
`best-effort-large`	4	16	No
`guaranteed-small`	2	4	Sí
`best-effort-small`	2	4	No

vSphere puede asignar cualquier cantidad de clases de máquinas virtuales existentes para que estén disponibles para los ingenieros de desarrollo y operaciones en un espacio de nombres específico.

La clase de máquina virtual proporciona una experiencia simplificada para los ingenieros de desarrollo y operaciones. Estos no necesitan comprender la configuración completa de cada máquina virtual que planean crear. En su lugar, pueden seleccionar una clase de máquina virtual entre las opciones disponibles, y el servicio de máquina virtual administra la configuración de la máquina virtual.

En el lado de Kubernetes, las clases de máquinas virtuales aparecen como recursos `VirtualMachineClass` y `VirtualMachineClassBinding`.

Imagen de máquina virtual

Una imagen de máquina virtual es una plantilla que contiene una configuración de software, que incluye un sistema operativo, aplicaciones y datos.

Cuando los ingenieros de desarrollo y operaciones crean máquinas virtuales, pueden seleccionar imágenes de la biblioteca de contenido asociada con el espacio de nombres. En desarrollo y operaciones, las imágenes se exponen como objetos de `VirtualMachineImage`.

El servicio de máquina virtual admite una cantidad limitada de imágenes de máquina virtual y sistemas operativos invitados. Las imágenes de máquina virtual compatibles aparecen en VMware Marketplace como OVF. Asegúrese de utilizar solo las imágenes de máquinas virtuales compatibles con el servicio de máquina virtual. Para buscar imágenes compatibles, busque la **`imagen del servicio de máquina virtual`** en el sitio web VMware Cloud Marketplace. Vea un ejemplo de la imagen del servicio de máquina virtual para CentOS en Imagen de servicio de máquina virtual para CentOS.

Origen del contenido

Un ingeniero de desarrollo y operaciones utiliza una biblioteca de contenido como origen de las imágenes para crear una máquina virtual. De forma similar a las clases de máquina virtual, un administrador de vSphere puede asignar bibliotecas de contenido existentes a un espacio de nombres para que estén disponibles para los ingenieros de desarrollo y operaciones.

Clase de almacenamiento

El servicio de máquina virtual utiliza clases de almacenamiento para colocar discos virtuales y asociar volúmenes persistentes de forma dinámica. Para obtener más información sobre las clases de almacenamiento, consulte Capítulo 10 Usar almacenamiento persistente en vSphere with Tanzu.

Especificación de la máquina virtual

Los ingenieros de desarrollo y operaciones describen el estado deseado de una máquina virtual en un archivo YAML que une la imagen de la máquina virtual, la clase de máquina virtual y la clase de almacenamiento.

Redes

El servicio de máquina virtual no tiene ningún requisito específico y se basa en la configuración de red disponible en vSphere with Tanzu. El servicio de máquina virtual es compatible con ambos tipos de redes: redes de vSphere o NSX-T. Cuando se implementan máquinas virtuales, un proveedor de red disponible asigna direcciones IP estáticas a las máquinas virtuales. Para obtener información, consulte Capítulo 4 Redes para vSphere with Tanzu.

Flujo de trabajo del administrador de vSphere para aprovisionar una máquina virtual

Como administrador de vSphere, debe establecer barreras para la directiva y el gobierno de las máquinas virtuales, y entregar recursos de máquina virtual, como clases de máquinas virtuales y plantillas de máquina virtual, a los ingenieros de desarrollo y operaciones. Después de implementar una máquina virtual, puede supervisarla mediante vSphere Client.

Paso	Descripción	Instrucciones
1	Cree y administre clases de máquinas virtuales.	■ Crear una clase de máquina virtual en vSphere with Tanzu ■ Para usar la vGPU de NVIDIA, configure un dispositivo PCI en la clase de máquina virtual. Consulte Agregar dispositivos PCI a una clase de máquina virtual en vSphere with Tanzu. ■ Editar o eliminar una clase de máquina virtual en vSphere with Tanzu
2	Asocie un conjunto de clases de máquinas virtuales con un espacio de nombres.	Asociar una clase de máquina virtual con un espacio de nombres en vSphere with Tanzu
3	Crear y administrar bibliotecas de contenido.	■ Para las máquinas virtuales independientes, consulte Crear y administrar bibliotecas de contenido para máquinas virtuales independientes en vSphere with Tanzu. ■ Para clústeres de Tanzu Kubernetes, consulte Crear y administrar bibliotecas de contenido para versiones de Tanzu Kubernetes.
4	Asocie una biblioteca de contenido con un espacio de nombres.	■ Para las máquinas virtuales independientes, consulte Asociar una biblioteca de contenido de máquina virtual con un espacio de nombres en vSphere with Tanzu. ■ Para clústeres de Tanzu Kubernetes, consulte Configurar un espacio de nombres de vSphere para las versiones de Tanzu Kubernetes.
5	Asocie las clases de almacenamiento con un espacio de nombres.	Creación y configuración de un espacio de nombres de vSphere
6	Supervise las máquinas virtuales implementadas.	Supervisar máquinas virtuales disponibles en vSphere with Tanzu

Flujo de trabajo de los ingenieros de desarrollo y operaciones para aprovisionar una máquina virtual

Los ingenieros de desarrollo y operaciones con permisos pueden revisar los recursos de máquina virtual disponibles e implementar máquinas virtuales en el espacio de nombres. Usan el comando `kubectl` para realizar las siguientes tareas.

Paso	Descripción	Instrucciones
1	Enumere las clases de máquinas virtuales, las imágenes y otros recursos asociados con el espacio de nombres.	Ver recursos de máquina virtual disponibles en un espacio de nombres en vSphere with Tanzu
2	Crear una máquina virtual	■ Para las máquinas virtuales independientes, consulte Implementar una máquina virtual en vSphere with Tanzu. ■ Para las máquinas virtuales del clúster de Tanzu Kubernetes, consulte Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS.

Este capítulo incluye los siguientes temas:

- Crear una clase de máquina virtual en vSphere with Tanzu
- Agregar dispositivos PCI a una clase de máquina virtual en vSphere with Tanzu
- Editar o eliminar una clase de máquina virtual en vSphere with Tanzu
- Asociar una clase de máquina virtual con un espacio de nombres en vSphere with Tanzu
- Administrar clases de máquinas virtuales en un espacio de nombres en vSphere with Tanzu
- Ver recursos de máquina virtual disponibles en un espacio de nombres en vSphere with Tanzu
- Implementar una máquina virtual en vSphere with Tanzu
- Supervisar máquinas virtuales disponibles en vSphere with Tanzu

Crear una clase de máquina virtual en vSphere with Tanzu

Como administrador de vSphere, cree clases de máquinas virtuales personalizadas que se usarán para una implementación de máquina virtual en un espacio de nombre en vSphere with Tanzu. Las clases de máquinas virtuales personalizadas pueden utilizarlas las máquinas virtuales independientes que se ejecutan en espacios de nombres y las máquinas virtuales que alojan un clúster de Tanzu Kubernetes.

Una clase de máquina virtual es una plantilla que define la CPU, la memoria y las reservas para las máquinas virtuales. La clase de máquina virtual ayuda a establecer barreras para la directiva y el gobierno de las máquinas virtuales, anticipando las necesidades de desarrollo y teniendo en cuenta las restricciones y la disponibilidad de recursos. vSphere with Tanzu ofrece varias clases de máquinas virtuales predeterminadas. Puede utilizarlas tal como están, editarlas o eliminarlas.

También puede crear clases de máquinas virtuales personalizadas. Al crear nuevas clases, tenga en cuenta las siguientes consideraciones.

- Las clases de máquinas virtuales que se crean en una instancia de vCenter Server están disponibles para todos los clústeres de vCenter Server y todos los espacios de nombres de estos clústeres.
- Las clases de máquinas virtuales están disponibles para todos los espacios de nombres de vCenter Server. Sin embargo, los ingenieros de desarrollo y operaciones pueden utilizar solo las clases de máquinas virtuales que se asocian con un espacio de nombres en particular.

Requisitos previos

Privilegios necesarios:

- **Espacio de nombres.Modificar configuración de todo el clúster**
- **Espacio de nombres.Modificar configuración del espacio de nombres**
- **Clases de máquinas virtuales.Administrar clases de máquinas virtuales**

Procedimiento

1 Desplácese a la página **Servicio de máquina virtual**.

   a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

   b Haga clic en la pestaña **Servicios** y haga clic en **Administrar** en el panel **Servicio de máquina virtual**.

2 En la página **Servicio de máquina virtual**, haga clic en **Clases de máquinas virtuales** y, a continuación, haga clic en **Crear clase de máquina virtual**.

3 En la página **Configuración**, especifique los atributos generales de la clase de máquina virtual.

Atributo de clase de máquina virtual	Descripción
Nombre	Identifica la clase de máquina virtual. Introduzca un nombre único conforme con DNS que cumpla estos requisitos: ■ Utilice un nombre único que no sea un duplicado de los nombres de las clases de máquinas virtuales predeterminadas o personalizadas de su entorno. ■ Utilice una cadena alfanumérica con una longitud máxima de 63 caracteres. ■ No utilice caracteres en mayúscula ni espacios. ■ Puede utilizar guiones en cualquier lugar, excepto como primer o último carácter. Por ejemplo, **`vm-class1`**. Después de crear la clase de máquina virtual, no puede cambiarle el nombre.
Recuento de vCPU	Define el número de CPU virtuales (vCPU) para una máquina virtual. Esta es una configuración de hardware de máquina virtual. Cuando un usuario de desarrollo y operaciones asigna la clase de máquina virtual a una máquina virtual, este recuento se convierte en el número configurado de vCPU para la máquina virtual.
Reserva de recursos de CPU	Parámetro opcional. Especifica la asignación de recursos de CPU mínima garantizada para una máquina virtual. Este valor se expresa en porcentaje (%). Si el valor es 0 %, no se define una reserva de CPU. El porcentaje que introduzca se multiplica por la CPU mínima disponible entre todos los nodos del clúster. El valor resultante, en MHz, especifica la cantidad de recursos de CPU que vSphere garantiza para una máquina virtual.
Memoria	Define la memoria configurada para una máquina virtual en MB, GB o TB. Esta es una configuración de hardware de máquina virtual. Cuando un usuario de desarrollo y operaciones asigna la directiva de clase de máquina virtual a una máquina virtual, esta recibe la cantidad de memoria definida por el atributo. El valor debe estar entre 4 MB y 24 TB, y ser múltiplo de 4 MB.
Reserva de recursos de memoria	Parámetro opcional. Define la cantidad reservada de memoria que está configurada para una máquina virtual. El valor del atributo oscila entre 0 y 100 %. Si agrega dispositivos PCI a la configuración de clase de máquina virtual, establezca el parámetro en 100 %.

4 (opcional) Para agregar dispositivos PCI, en la página **Configuración**, seleccione **Sí** en el menú desplegable **Dispositivos PCI** y haga clic en **Siguiente**.

   Si selecciona esta opción, el valor de reserva de recursos de memoria cambia automáticamente al 100 %.

   Para conocer los requisitos y los detalles adicionales, consulte Agregar dispositivos PCI a una clase de máquina virtual en vSphere with Tanzu.

5 En la página **Revisar y Confirmar**, revise los detalles y haga clic en **Finalizar**.

Pasos siguientes

Después de crear una clase de máquina virtual, puede editar sus parámetros o eliminarla del entorno. Consulte Editar o eliminar una clase de máquina virtual en vSphere with Tanzu.

Para que la clase de máquina virtual esté disponible para los ingenieros de desarrollo y operaciones, asóciela con un espacio de nombres. La asociación de la clase de máquina virtual se produce por espacio de nombres. Consulte Asociar una clase de máquina virtual con un espacio de nombres en vSphere with Tanzu.

Atributos de las clases de máquina virtual en vSphere with Tanzu

Como administrador de vSphere, puede crear o editar las clases de máquinas virtuales (VM) que utilizan las máquinas virtuales de un espacio de nombres de vSphere. Para cada clase de máquina virtual, especifique un subconjunto de atributos disponibles.

En la siguiente tabla se enumeran todos los atributos que puede definir dentro de una clase de máquina virtual.

Atributo de clase de máquina virtual	Descripción
Nombre	Identifica la clase de máquina virtual. Introduzca un nombre único conforme con DNS que cumpla estos requisitos: ■ Utilice un nombre único que no sea un duplicado de los nombres de las clases de máquinas virtuales predeterminadas o personalizadas de su entorno. ■ Utilice una cadena alfanumérica con una longitud máxima de 63 caracteres. ■ No utilice caracteres en mayúscula ni espacios. ■ Puede utilizar guiones en cualquier lugar, excepto como primer o último carácter. Por ejemplo, **`vm-class1`**. Después de crear la clase de máquina virtual, no puede cambiarle el nombre.
Recuento de vCPU	Define el número de CPU virtuales (vCPU) para una máquina virtual. Esta es una configuración de hardware de máquina virtual. Cuando un usuario de desarrollo y operaciones asigna la clase de máquina virtual a una máquina virtual, este recuento se convierte en el número configurado de vCPU para la máquina virtual.

Atributo de clase de máquina virtual	Descripción
Reserva de recursos de CPU	Parámetro opcional. Especifica la asignación de recursos de CPU mínima garantizada para una máquina virtual. Este valor se expresa en porcentaje (%). Si el valor es 0 %, no se define una reserva de CPU. El porcentaje que introduzca se multiplica por la CPU mínima disponible entre todos los nodos del clúster. El valor resultante, en MHz, especifica la cantidad de recursos de CPU que vSphere garantiza para una máquina virtual.
Memoria	Define la memoria configurada para una máquina virtual en MB, GB o TB. Esta es una configuración de hardware de máquina virtual. Cuando un usuario de desarrollo y operaciones asigna la directiva de clase de máquina virtual a una máquina virtual, esta recibe la cantidad de memoria definida por el atributo. El valor debe estar entre 4 MB y 24 TB, y ser múltiplo de 4 MB.
Reserva de recursos de memoria	Parámetro opcional. Define la cantidad reservada de memoria que está configurada para una máquina virtual. El valor del atributo oscila entre 0 y 100 %. Si agrega dispositivos PCI a la configuración de clase de máquina virtual, establezca el parámetro en 100 %.

Agregar dispositivos PCI a una clase de máquina virtual en vSphere with Tanzu

Si los hosts ESXi de su entorno de vSphere with Tanzu tienen uno o varios dispositivos de gráficos de GPU NVIDIA GRID, es posible configurar las máquinas virtuales para que usen esta tecnología de GPU virtual (vGPU) NVIDIA GRID. También se pueden configurar otros dispositivos PCI en un host ESXi para que estén disponibles para una máquina virtual en modo de acceso directo.

GPU NVIDIA GRID

Los dispositivos de gráficos de GPU NVIDIA GRID están diseñados para optimizar operaciones gráficas complejas y permitir que estas se ejecuten con un alto rendimiento sin sobrecargar la CPU. La unidad de vGPU NVIDIA GRID brinda un rendimiento de gráficos sin igual, economía y escalabilidad, ya que permite compartir una sola GPU física entre varias máquinas virtuales como si fueran dispositivos de acceso directo habilitados para vGPU distintos.

Cuando configura NVIDIA vGPU para una máquina virtual, se agrega un dispositivo PCI para vGPU a una clase de máquina virtual.

Las siguientes consideraciones se aplican cuando se utiliza NVIDIA vGPU:

- Las máquinas virtuales con dispositivos vGPU administradas por el servicio de máquina virtual se apagan automáticamente cuando un host ESXi entra en modo de mantenimiento. Esto puede afectar temporalmente a las cargas de trabajo que se ejecutan en las máquinas virtuales. Las máquinas virtuales se encienden automáticamente después de que el host sale del modo de mantenimiento.

Instancia dinámica de DirectPath I/O

Mediante la instancia dinámica de DirectPath I/O, la máquina virtual puede acceder directamente a los dispositivos PCI y PCIe físicos conectados a un host.

Puede usar la instancia dinámica de DirectPath I/O para asignar varios dispositivos de acceso directo a PCI a una máquina virtual. Cada dispositivo de acceso directo se puede especificar mediante su proveedor de PCI e identificador de dispositivo.

Requisitos previos

- Compruebe que la máquina host sea compatible según la Guía de Compatibilidad de VMware y póngase en contacto con el proveedor para comprobar que el host cumpla con los requisitos de alimentación y configuración. Instale un dispositivo PCI en el host ESXi.
- Para configurar NVIDIA vGPU, siga estos requisitos previos:
  - Use vSphere versión 7.0 Update 3 o una versión posterior.
  - Configure los ajustes de los gráficos de hosts ESXi con al menos un dispositivo en modo **Compartidos directos**. Consulte Configuración de gráficos de host.
  - Instale el software NVIDIA vGPU. NVIDIA proporciona un paquete de software vGPU que incluye los siguientes componentes.

    Para obtener más información, consulte la documentación correspondiente del software NVIDIA Virtual GPU.
    - vGPU Manager que un administrador de vSphere instala en el host ESXi. Consulte el artículo 2033434 de la base de conocimientos de VMware.
    - Controlador de máquina virtual invitado que un ingeniero de desarrollo y operaciones instala en la máquina virtual después de implementar y arrancar la máquina virtual. Consulte Instalar el controlador invitado de NVIDIA en una máquina virtual en vSphere with Tanzu.
- Para configurar una instancia dinámica de DirectPath I/O para dispositivos de acceso directo a PCI, siga estos requisitos previos:
  - Utilice vSphere versión 7.0 Update 3 MP01.
  - Conecte los dispositivos PCI al host y márquelos como disponibles para el acceso directo. Consulte Marcar un dispositivo PCI como acceso directo.

- Privilegios necesarios:
  - **Espacio de nombres.Modificar configuración de todo el clúster**
  - **Espacio de nombres.Modificar configuración del espacio de nombres**
  - **Clases de máquinas virtuales.Administrar clases de máquinas virtuales**

Procedimiento

1 Agregue un dispositivo PCI a una clase de máquina virtual cuando cree o edite una clase de máquina virtual existente.

Opción	Acción
Crear una nueva clase de máquina virtual	a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**. b Haga clic en la pestaña **Servicios** y haga clic en **Administrar** en el panel **Servicio de máquina virtual**. c En la página **Servicio de máquina virtual**, haga clic en **Clases de máquinas virtuales** y, a continuación, haga clic en **Crear clase de máquina virtual**. d En la página **Configuración**, especifique los atributos generales de la clase de máquina virtual. Consulte Atributos de las clases de máquina virtual en vSphere with Tanzu. Asegúrese de que el valor de reserva de recursos de memoria esté establecido en 100 %. e Para agregar dispositivos PCI, en la página **Configuración**, seleccione **Sí** en el menú desplegable **Dispositivos PCI** y haga clic en **Siguiente**.
Edite una clase de máquina virtual.	a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**. b Haga clic en la pestaña **Servicios** y haga clic en **Administrar** en el panel **Servicio de máquina virtual**. c En la página **Servicio de máquina virtual**, haga clic en **Clases de máquinas virtuales**. d En el panel de la clase de máquina virtual seleccionada, haga clic en **Administrar** y, luego, en **Editar**. Asegúrese de que el valor de reserva de recursos de memoria esté establecido en 100 %. e Para agregar dispositivos PCI, en la página **Configuración**, seleccione **Sí** en el menú desplegable **Dispositivos PCI** y haga clic en **Siguiente**.

2 En la página **Dispositivos PCI**, expanda el menú **Agregar dispositivo PCI**, seleccione el tipo de acceso y otras opciones correspondientes, y haga clic en **Siguiente**.

Opción	Acción
NVIDIA GRID vGPU	Especifique las siguientes opciones: ■ **Modelo**. Nombre del dispositivo físico. Seleccione el dispositivo de la lista de dispositivos disponibles en el host. ■ **Uso compartido de GPU**. Indica cómo se comparte la GPU física entre las máquinas virtuales. Por ejemplo, **Tiempo Compartido** ■ **Modo GPU**. El modo GPU dentro de una máquina virtual. Por ejemplo, **Informático** es una configuración optimizada para aplicaciones informáticas de alto rendimiento. Mientras que **Estación de trabajo** se utiliza para cargas de trabajo de uso intensivo de gráficos. ■ **Memoria de GPU**. Memoria de GPU mínima en GB por máquina virtual. ■ **Número de vGPU**. Número de dispositivos vGPU por máquina virtual.
Instancia dinámica de DirectPath I/O	En la lista **Dispositivo PCI**, seleccione los dispositivos de acceso directo a PCI por proveedor, nombre de modelo o etiqueta de hardware.

3 En la página **Revisar y Confirmar**, revise los detalles y haga clic en **Finalizar**.

Resultados

Una etiqueta **GPU** en el panel de clase de máquina virtual indica que la clase de máquina virtual está habilitada para GPU.

Editar o eliminar una clase de máquina virtual en vSphere with Tanzu

Como administrador de vSphere, puede crear clases de máquinas virtuales personalizadas para las máquinas virtuales en un espacio de nombres de vSphere. Después de crear una clase de máquina virtual, puede editar sus parámetros. También puede editar las clases de máquinas virtuales predeterminadas que ofrece vSphere with Tanzu. Si ya no necesita una clase de máquina virtual existente, puede eliminarla del entorno.

La edición de una clase de máquina virtual no da como resultado la reconfiguración automática de las máquinas virtuales que se implementaron previamente a partir de esta clase. Por ejemplo, si un usuario de desarrollo y operaciones creó un clúster de Tanzu Kubernetes con una clase de máquina virtual y, posteriormente, usted cambia la definición de esa clase, las máquinas virtuales de Tanzu Kubernetes existentes no se verán afectadas. Las nuevas máquinas virtuales de Tanzu Kubernetes utilizarán la definición de clase modificada.

Precaución Si se escala horizontalmente un clúster de Tanzu Kubernetes después de editar una clase de máquina virtual utilizada por ese clúster, los nuevos nodos del clúster utilizan la definición de clase actualizada, pero los nodos del clúster existentes siguen usando la definición de clase inicial, lo que provoca un error de coincidencia. Tanto los nodos de plano de control como los nodos de trabajo pueden escalarse. Para obtener información sobre el escalado, consulte Escalar un clúster de Tanzu Kubernetes mediante la API v1alpha1 de servicio Tanzu Kubernetes Grid.

Cuando se elimina una clase de máquina virtual, se la elimina de todos los espacios de nombres asociados. Los usuarios de desarrollo y operaciones ya no pueden usar esa clase de máquina virtual para realizar el autoservicio de las máquinas virtuales. Las máquinas virtuales que ya se crearon con esa clase de máquina virtual no se ven afectadas.

Requisitos previos

- Compruebe que tiene al menos una clase de máquina virtual. Consulte Crear una clase de máquina virtual en vSphere with Tanzu.
- Privilegios necesarios:
  - **Espacio de nombres.Modificar configuración de todo el clúster**
  - **Espacio de nombres.Modificar configuración del espacio de nombres**
  - **Clases de máquinas virtuales.Administrar clases de máquinas virtuales**

Procedimiento

1 En vSphere Client, muestre las clases de máquinas virtuales disponibles.

   a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

   b Haga clic en la pestaña **Servicios** y haga clic en el panel **Servicio de máquina virtual**.

   c En la página **Servicio de máquina virtual**, haga clic en **Clases de máquinas virtuales**.

   Todas las clases de máquinas virtuales predeterminadas o creadas por el usuario aparecen en **Clases de máquinas virtuales disponibles**.

2 Edite o elimine una clase de máquina virtual existente.

Opción	Descripción
Edite una clase de máquina virtual.	a En el panel de la clase de máquina virtual seleccionada, haga clic en **Administrar** y, luego, en **Editar**. b Modifique los parámetros de la clase de máquina virtual. Consulte Atributos de las clases de máquina virtual en vSphere with Tanzu. **Nota** No puede cambiar el nombre de la clase de máquina virtual.
Eliminar una clase de máquina virtual	a En el panel de la clase de máquina virtual seleccionada, haga clic en **Administrar** y, luego, en **Eliminar**. b Confirme que desea eliminar la clase de máquina virtual.

Pasos siguientes

Para que una clase de máquina virtual esté disponible para los ingenieros de desarrollo y operaciones, asóciela con un espacio de nombres. La asociación de la clase de máquina virtual se produce por espacio de nombres. Consulte Asociar una clase de máquina virtual con un espacio de nombres en vSphere with Tanzu.

Asociar una clase de máquina virtual con un espacio de nombres en vSphere with Tanzu

Como administrador de vSphere, puede agregar una clase de máquina virtual a uno o varios espacios de nombres en un clúster supervisor. Cuando se agrega una clase de máquina virtual a un espacio de nombres, la clase queda disponible para los usuarios de desarrollo y operaciones, para que puedan iniciar máquinas virtuales de autoservicio en el entorno del espacio de nombres de Kubernetes. Las clases de máquinas virtuales que usted asigna al espacio de nombres también las utilizan las máquinas virtuales que conforman los clústeres de Tanzu Kubernetes.

Puede agregar varias clases de máquinas virtuales a un único espacio de nombres. Las diferentes clases de máquinas virtuales sirven como indicadores de diferentes niveles de servicio. Si publica varias clases de máquinas virtuales, los usuarios de desarrollo y operaciones pueden seleccionar entre todas las clases personalizadas y predeterminadas al crear y administrar máquinas virtuales en el espacio de nombres.

Nota Para poder implementar un clúster de Tanzu Kubernetes en un espacio de nombres recién creado, los ingenieros de desarrollo y operaciones deben tener acceso a las clases de máquinas virtuales. Como administrador de vSphere, debe asociar explícitamente las clases de máquinas virtuales predeterminadas o personalizadas a cualquier nuevo espacio de nombres donde se implemente el clúster de Tanzu Kubernetes. Los espacios de nombres existentes, donde ya se aprovisionaron los clústeres de Tanzu Kubernetes, siguen teniendo acceso automático a las clases de máquinas virtuales predeterminadas. Sin embargo, también puede asociar clases de máquinas virtuales personalizadas con cualquier espacio de nombres existente.

Requisitos previos

Utilice las clases de máquinas virtuales predeterminadas que VMware proporciona o cree nuevas clases. Consulte Crear una clase de máquina virtual en vSphere with Tanzu.

Privilegios necesarios:

- **Espacio de nombres.Modificar configuración de todo el clúster**
- **Espacio de nombres.Modificar configuración del espacio de nombres**
- **Clases de máquinas virtuales.Administrar clases de máquinas virtuales**

Procedimiento

1. En vSphere Client, vaya al espacio de nombres.
   a. En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.
   b. Haga clic en la pestaña **Espacios de nombres** y haga clic en el espacio de nombres.
2. Agregue una clase de máquina virtual.
   a. En el panel **Servicio de máquina virtual**, haga clic en **Agregar clase de máquina virtual**.
   b. Seleccione una o varias clases de máquinas virtuales y haga clic en **Aceptar**.

Resultados

Las clases de máquinas virtuales que agregó quedan disponibles en el espacio de nombres para que desarrollo y operaciones realice el autoservicio de las máquinas virtuales. Estas clases también las pueden utilizar las máquinas virtuales que conforman los clústeres de Tanzu Kubernetes.

Pasos siguientes

Después de asociar una clase de máquina virtual con un espacio de nombres, puede agregar más clases de máquinas virtuales o eliminar la clase para cancelar su publicación en el espacio de nombres. Consulte Administrar clases de máquinas virtuales en un espacio de nombres en vSphere with Tanzu.

Administrar clases de máquinas virtuales en un espacio de nombres en vSphere with Tanzu

Como administrador de vSphere, puede asociar una clase de máquina virtual con uno o varios espacios de nombres en un clúster supervisor. Después de asociar una clase de máquina virtual con un espacio de nombres, puede agregar más clases de máquinas virtuales o eliminar la clase para cancelar su publicación en el espacio de nombres de Kubernetes.

Requisitos previos

- Compruebe que al menos una clase de máquina virtual esté asociada con el espacio de nombres. Consulte Asociar una clase de máquina virtual con un espacio de nombres en vSphere with Tanzu.
- Si desea quitar una clase de máquina virtual de un espacio de nombres, compruebe que servicio Tanzu Kubernetes Grid no la utilice. Su eliminación puede afectar las operaciones de servicio Tanzu Kubernetes Grid.
- Privilegios necesarios:
  - **Espacio de nombres.Modificar configuración de todo el clúster**
  - **Espacio de nombres.Modificar configuración del espacio de nombres**
  - **Clases de máquinas virtuales.Administrar clases de máquinas virtuales**

Procedimiento

1 En vSphere Client, vaya al espacio de nombres.

   a En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

   b Haga clic en la pestaña **Espacios de nombres** y haga clic en el espacio de nombres.

2 Agregue o elimine una clase de máquina virtual.

a En el panel **Servicio de máquina virtual**, haga clic en **Administrar clase de máquina virtual**.

b Realice una de las siguientes operaciones.

Opción	Descripción
Quitar una clase de máquina virtual	Anule la selección de la clase de máquina virtual y haga clic en **Aceptar**.
Agregar una clase de máquina virtual	Seleccione una o varias clases de máquinas virtuales y haga clic en **Aceptar**.

Ver recursos de máquina virtual disponibles en un espacio de nombres en vSphere with Tanzu

Para poder implementar una máquina virtual independiente en vSphere with Tanzu, un ingeniero de desarrollo y operaciones debe tener acceso a recursos específicos de la máquina virtual. Como ingeniero de desarrollo y operaciones, compruebe que puede acceder a estos recursos y ver las clases y las plantillas de máquina virtual disponibles en su entorno. También puede enumerar las clases de almacenamiento y otros elementos que podría necesitar para realizar el autoservicio de una máquina virtual.

Esta tarea abarca los comandos que se utilizan para acceder a los recursos disponibles para la implementación de una máquina virtual independiente. Para obtener información sobre los recursos necesarios para implementar clústeres de Tanzu Kubernetes y las máquinas virtuales que conforman los clústeres, consulte Clases de máquina virtual para clústeres de Tanzu Kubernetes.

Requisitos previos

Un administrador de vSphere ha realizado estos pasos:

- Se creó un espacio de almacenamiento y se asoció con directivas de almacenamiento. Consulte Creación y configuración de un espacio de nombres de vSphere.
- Clases de máquina virtual predeterminadas o personalizadas asociadas con un espacio de nombres. Consulte Asociar una clase de máquina virtual con un espacio de nombres en vSphere with Tanzu.
- Se creó una biblioteca de contenido y se asoció con un espacio de nombres. Consulte Asociar una biblioteca de contenido de máquina virtual con un espacio de nombres en vSphere with Tanzu.

  Nota Si una biblioteca de contenido está protegida por una directiva de seguridad, todos los elementos de la biblioteca deben ser compatibles. Si una biblioteca protegida incluye una combinación de elementos conformes y no conformes, el comando `kubectl get virtualmachineimages` no puede presentar imágenes de máquina virtual a los ingenieros de desarrollo y operaciones.

Procedimiento

1 Acceda al espacio de nombres en el entorno de Kubernetes.

Consulte Obtener y utilizar el contexto del clúster supervisor.

2 Para ver las clases de máquina virtual disponibles en el espacio de nombres, ejecute el siguiente comando.

`kubectl get virtualmachineclassbindings`

Es posible que se muestre el siguiente resultado.

Nota Debido a que el tipo de clase de máquina virtual de mejor esfuerzo permite que los recursos se sobreasignen, puede quedarse sin recursos si ha establecido límites en el espacio de nombres en el que está aprovisionando las máquinas virtuales. Por este motivo, utilice el tipo de clase de máquina virtual garantizada en el entorno de producción.

```
NAME                      VIRTUALMACHINECLASS       AGE

best-effort-large         best-effort-large         44m
best-effort-medium        best-effort-medium        44m
best-effort-small         best-effort-small         44m
best-effort-xsmall        best-effort-xsmall        44m
custom                    custom                    44m
```

3 Para ver los detalles de una clase de máquina virtual específica, ejecute los siguientes comandos.

- `kubectl describe virtualmachineclasses` *name_vm_class*

  Si una clase de máquina virtual incluye un dispositivo vGPU, puede ver su perfil en `spec: hardware: devices: vgpuDevices`.

```
......
spec:
  hardware:
    cpus: 4
    devices:
      vgpuDevices:
      - profileName: grid_v100-q4
......
```

- `kubectl get virtualmachineclasses -o wide`

  Si la clase de máquina virtual incluye una vGPU o un directo de acceso directo, el resultado lo muestra en la columna `VGPUDevicesProfileNames` o `PassthroughDeviceIDs`.

4 Ver las imágenes de máquina virtual.

`kubectl get virtualmachineimages`

El resultado que ve es similar al siguiente.

```
NAME                                                VERSION  OSTYPE                FORMAT
IMAGESUPPORTED  AGE
centos-stream-8-vmservice-v1alpha1-xxxxxxxxxxxxx             centos8_64Guest       ovf
true            4d3h
```

5 Para describir una imagen específica, utilice el siguiente comando.

```
kubectl describe virtualmachineimage/centos-stream-8-vmservice-v1alpha1-
xxxxxxxxxxxxx
```

Las máquinas virtuales con dispositivos de vGPU requieren imágenes que tengan el modo de arranque establecido en EFI, como CentOS. Asegúrese de tener acceso a estas imágenes. Si desea información sobre imágenes compatibles, busque la **imagen del servicio de máquina virtual** en el sitio web VMware Cloud Marketplace.

6 Compruebe si puede acceder a las clases de almacenamiento.

```
kubectl get resourcequotas
```

Para obtener más información, consulte Mostrar clases de almacenamiento en un espacio de nombres de vSphere o clúster de Tanzu Kubernetes.

```
NAME                         AGE
REQUEST
     LIMIT
my-ns-ubuntu-storagequota    24h   wcpglobal-storage-profile.storageclass.storage.k8s.io/
requests.storage: 0/9223372036854775807
```

7 Si utiliza vSphere Distributed Switch para las redes de carga de trabajo, obtenga el nombre de la red.

Nota Utilice esta información para especificar el parámetro `networkName` en el archivo YAML de la máquina virtual cuando `networkType` sea **vsphere-distributed**. No es necesario obtener ni especificar el nombre de red si utiliza VMware NSX-T.

```
kubectl get network
```

```
NAME      AGE
primary   7d2h
```

Pasos siguientes

Ahora puede implementar máquinas virtuales. Consulte Implementar una máquina virtual en vSphere with Tanzu.

Implementar una máquina virtual en vSphere with Tanzu

Como ingeniero de desarrollo y operaciones, puede aprovisionar una máquina virtual y su SO invitado de forma declarativa al escribir especificaciones de implementación de máquina virtual en un archivo YAML de Kubernetes.

Requisitos previos

- Compruebe si dispone de recursos para implementar una máquina virtual en el espacio de nombres. Consulte Ver recursos de máquina virtual disponibles en un espacio de nombres en vSphere with Tanzu.
- Si utiliza vGPU de NVIDIA u otros dispositivos PCI para sus máquinas virtuales, se aplican las siguientes consideraciones:
  - Asegúrese de utilizar la clase de máquina virtual adecuada con la configuración de PCI. Consulte Agregar dispositivos PCI a una clase de máquina virtual en vSphere with Tanzu.
  - Las máquinas virtuales con dispositivos de vGPU requieren imágenes que tengan el modo de arranque establecido en EFI, como CentOS. Asegúrese de tener acceso a estas imágenes. Si desea información sobre imágenes compatibles, busque la **`imagen del servicio de máquina virtual`** en el sitio web VMware Cloud Marketplace.
  - Las máquinas virtuales con dispositivos vGPU administradas por el servicio de máquina virtual se apagan automáticamente cuando un host ESXi entra en modo de mantenimiento. Esto puede afectar temporalmente a las cargas de trabajo que se ejecutan en las máquinas virtuales. Las máquinas virtuales se encienden automáticamente después de que el host sale del modo de mantenimiento.

Procedimiento

1 Prepare el archivo YAML de la máquina virtual.

En el archivo, especifique los siguientes parámetros:

Opción	Descripción
apiVersion	Especifica la versión de la API del servicio de máquina virtual. Por ejemplo, **`vmoperator.vmware.com/v1alpha1`**.
kind	Especifica el tipo de recurso de Kubernetes que se debe crear. El único valor disponible es **`VirtualMachine`**.
spec.imageName	Especifica la imagen de la biblioteca de contenido que debe utilizar la máquina virtual. Por ejemplo, **`centos-stream-8-vmservice-v1alpha1-xxxxxxxxxxxxx`**.
spec.storageClass	Identifica la clase de almacenamiento que se utilizará para el almacenamiento de los volúmenes persistentes. Por ejemplo, **`wcpglobal-storage-profile`**.
spec.className	Especifica el nombre de la clase de máquina virtual que describe la configuración de hardware virtual que se utilizará. Por ejemplo, **`custom`**.

Opción	Descripción
spec.networkInterfaces	Especifica la configuración relacionada con la red para la máquina virtual. ■ `networkType`. Los valores para esta clave pueden ser **`nsx-t`** o **`vsphere-distributed`**. ■ `networkName`. Especifique el nombre solo si `networkType` es **`vsphere-distributed`**. Puede obtener esta información mediante el comando `kubectl get network`. Si `networkType` es **`nsx-t`**, no es necesario que indique `networkName`.
spec.vmMetadata	Incluye metadatos adicionales que se transferirán a la máquina virtual. Puede utilizar esta clave para personalizar la imagen del SO invitado y establecer estos elementos como el `hostname` de la máquina virtual y `user-data`, incluidas las contraseñas, las claves SSH, etc. El YAML de ejemplo siguiente utiliza `ConfigMap` para almacenar los metadatos.

Utilice lo siguiente como ejemplo de un archivo YAML `vmsvc-centos-vm.yaml`.

```
apiVersion: vmoperator.vmware.com/v1alpha1
kind: VirtualMachine
metadata:
  name: vmsvc-centos-vm
  namespace: my-ns-centos
spec:
  imageName: centos-stream-8-vmservice-v1alpha1-xxxxxxxxxxxxx
  className: custom
  powerState: poweredOn
  storageClass: wcpglobal-storage-profile
  networkInterfaces:
  - networkName: primary
    networkType: vsphere-distributed
  vmMetadata:
      configMapName: vmsvc-centos-nginx-cm
      transport: OvfEnv
---
apiVersion: v1
kind: ConfigMap
metadata:
    name: vmsvc-centos-nginx-cm
    namespace: my-ns-centos
data:
  user-data: >-

I2Nsb3VkLWNvbmZpZwoKcGFzc3dvcmQ6IFZNV0FSRQpzc2hfcHdhdXRoOiB0cnVlCgp1c2VyczoKICAtIG5hbWU6IHZ
td2FyZQogICAgc3VkbzogQUxMPShBTEwpIE5PUEFTU1dEOkFMTAogICAgbG9ja19wYXNzd2Q6IGZhbHNlCiAgICAjIF
Bhc3N3b3JkIHNldCB0byBBZG1pbiEyMwogICAgcGFzc3dkOiAnJDEkc2FsdCRTT0MzM2ZWYkEvWnhlSXdENXl3MXUxJ
wogICAgc2hlbGw6IC9iaW4vYmFzaAoKd3JpdGVfZmlsZXM6CiAgLSBjb250ZW50OiB8CiAgICAgIFZNU1ZDIFNheXMg
SGVsbG8gV29ybGQKICAgIHBhdGg6IC9oZWxsb3dvcmxkCg==
```

ConfigMap contiene el blob de cloud-config que especifica el nombre de usuario y la contraseña del SO invitado. En este ejemplo, user-data en vmsvc-centos-nginx-cm, ConfigMap representa el siguiente fragmento de código en formato base64:

```
#cloud-config
password: VMWARE
ssh_pwauth: true
users:
  - name: vmware
    sudo: ALL=(ALL) NOPASSWD:ALL
    lock_passwd: false
    passwd: '$1$salt$SOC33fVbA/ZxeIwD5yw1u1'
    shell: /bin/bash
write_files:
  - content: |
      VMSVC Says Hello World
    path: /helloworld
```

Para obtener más información sobre las especificaciones de cloud-config, consulte https://cloudinit.readthedocs.io/en/latest/topics/examples.html.

2 Implemente la máquina virtual.

```
kubectl apply -f vmsvc-centos-vm.yaml
```

3 Compruebe que se haya creado la máquina virtual.

```
kubectl get vm -n my-ns-centos
NAME                AGE
vmsvc-centos-vm     28s
```

4 Compruebe el estado de la máquina virtual y los eventos asociados.

```
kubectl describe virtualmachine vmsvc-centos-vm
```

Los resultados son similares al siguiente. De los resultados también puede obtener la dirección IP de la máquina virtual, que aparece en el campo Vm Ip.

```
Name:          vmsvc-centos-vm
Namespace:     my-ns-centos
Annotations:   vmoperator.vmware.com/image-supported-check: disabled
API Version:   vmoperator.vmware.com/v1alpha1
Kind:          VirtualMachine
Metadata:
  Creation Timestamp:  2021-03-23T19:07:36Z
  Finalizers:
    virtualmachine.vmoperator.vmware.com
  Generation:  1
  Managed Fields:
 ...
 ...
Spec:
  Class Name:  custom
```

```
  Image Name:  vmservice-centos-20-10-server-cloudimg-amd64
  Network Interfaces:
    Network Name:  primary
    Network Type:  vsphere-distributed
  Power State:     poweredOn
  Storage Class:   wcpglobal-storage-profile
  Vm Metadata:
    Config Map Name:  vmsvc-centos-nginx-cm
    Transport:        OvfEnv
Status:
  Bios UUID:              4218ec42-aeb3-9491-fe22-19b6f954ce38
  Change Block Tracking:  false
  Conditions:
    Last Transition Time:  2021-03-23T19:08:59Z
    Status:                True
    Type:                  VirtualMachinePrereqReady
  Host:                    10.185.240.10
  Instance UUID:           50180b3a-86ee-870a-c3da-90ddbaffc950
  Phase:                   Created
  Power State:             poweredOn
  Unique ID:               vm-73
  Vm Ip:                   10.161.75.162
Events:                    <none>
...
```

5 Compruebe que se pueda acceder a la IP de la máquina virtual.

```
ping 10.161.75.162
PING 10.161.75.162 (10.161.75.162): 56 data bytes
64 bytes from 10.161.75.162: icmp_seq=0 ttl=59 time=43.528 ms
64 bytes from 10.161.75.162: icmp_seq=1 ttl=59 time=53.885 ms
64 bytes from 10.161.75.162: icmp_seq=2 ttl=59 time=31.581 ms
```

Resultados

Una máquina virtual creada a través del servicio de máquina virtual solo puede administrarla desarrollo y operaciones desde el espacio de nombres de Kubernetes. Su ciclo de vida no puede administrarse desde vSphere Client, pero los administradores de vSphere pueden supervisar la máquina virtual y sus recursos. Para obtener más información, consulte Supervisar máquinas virtuales disponibles en vSphere with Tanzu.

Pasos siguientes

Para obtener más información, consulte el blog Introducción al aprovisionamiento de máquinas virtuales.

Si la máquina virtual incluye un dispositivo PCI configurado para vGPU, instale el controlador de pantalla NVIDIA. Consulte Instalar el controlador invitado de NVIDIA en una máquina virtual en vSphere with Tanzu.

Instalar el controlador invitado de NVIDIA en una máquina virtual en vSphere with Tanzu

Después de crear y arrancar una máquina virtual en el entorno de vSphere with Tanzu, instale el controlador de gráficos NVIDIA vGPU en la máquina virtual para habilitar completamente el funcionamiento de la GPU.

Requisitos previos

- Cree una máquina virtual con el dispositivo NVIDIA vGPU. La máquina virtual debe hacer referencia a la clase de máquina virtual que incluye una definición de vGPU. Consulte Agregar dispositivos PCI a una clase de máquina virtual en vSphere with Tanzu.
- Compruebe que descargó el paquete de software de vGPU del sitio de descargas de NVIDIA, descomprimió el paquete y tiene listo el componente de la unidad de invitado. Para obtener información, consulte la documentación correspondiente del software de GPU virtual de NVIDIA.

  Nota La versión del componente del controlador debe corresponder a la versión de vGPU Manager que un administrador de vSphere instaló en el host ESXi. Consulte Agregar dispositivos PCI a una clase de máquina virtual en vSphere with Tanzu.

Procedimiento

1 Copie el paquete de controladores Linux del software de NVIDIA vGPU, por ejemplo, `NVIDIA-Linux-x86_64-` *`versión`* `-grid.run`, en la máquina virtual invitada.

2 Antes de intentar ejecutar el instalador del controlador, finalice todas las aplicaciones.

3 Inicie el instalador del controlador NVIDIA vGPU.

```
sudo ./NVIDIA-Linux-x86_64-version-grid.run
```

4 Acepte el acuerdo de licencia de software de NVIDIA y seleccione **Sí** para actualizar automáticamente los ajustes de configuración de X.

5 Compruebe que se haya instalado el controlador.

Por ejemplo:

```
~$ nvidia-smi
Wed May 19 22:15:04 2021
+-----------------------------------------------------------------------------+
| NVIDIA-SMI 460.63       Driver Version: 460.63       CUDA Version: 11.2     |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|                               |                      |               MIG M. |
|===============================+======================+======================|
|   0  GRID V100-4Q        On   | 00000000:02:00.0 Off |                  N/A|
| N/AN/AP0    N/A/  N/A|    304MiB /  4096MiB |      0%      Default |
|                               |                      |                  N/A|
```

```
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                                  |
|  GPU   GI   CI        PID   Type   Process name                  GPU Memory |
|        ID   ID                                                   Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
```

Supervisar máquinas virtuales disponibles en vSphere with Tanzu

Como administrador de vSphere, utilice vSphere Client para supervisar una máquina virtual implementada por Desarrollo y operaciones en el entorno de Kubernetes.

No se puede administrar el ciclo de vida de la máquina virtual desde vSphere Client.

Requisitos previos

Un ingeniero de Desarrollo y operaciones implementó una máquina virtual. Consulte Implementar una máquina virtual en vSphere with Tanzu.

Procedimiento

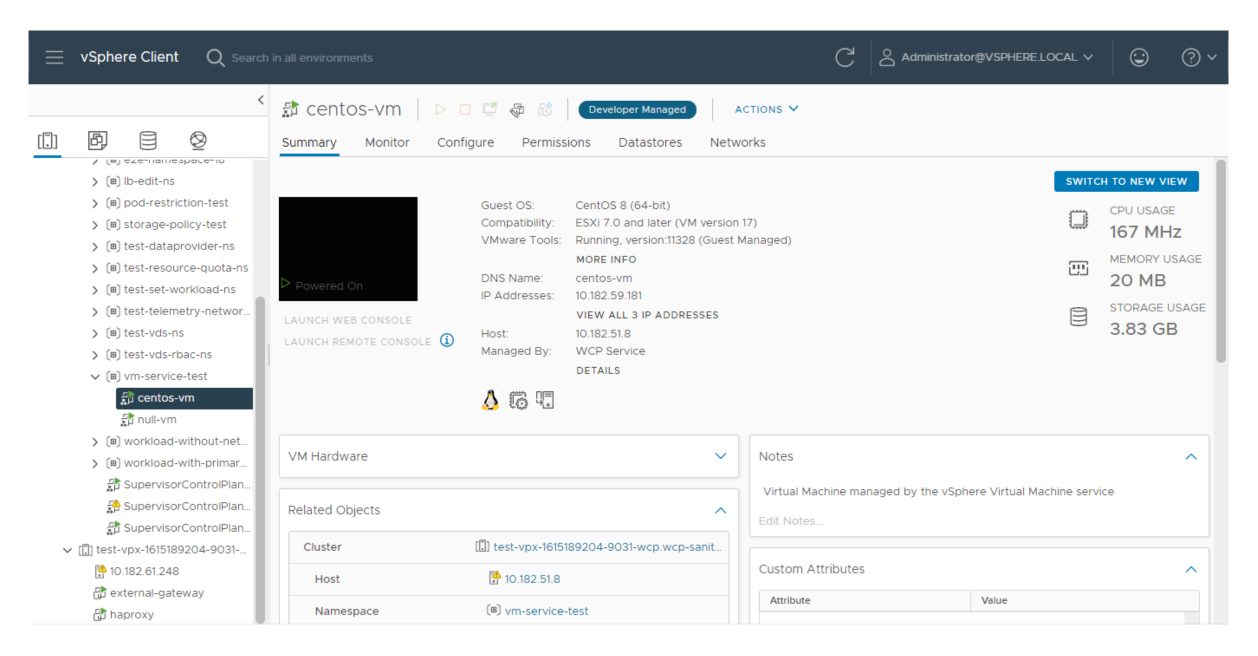
1 En el vSphere Client, desplácese hasta el clúster de host que tiene vSphere with Tanzu habilitado.

2 En **Espacios de nombres**, expanda el espacio de nombres donde se implementó una máquina virtual.

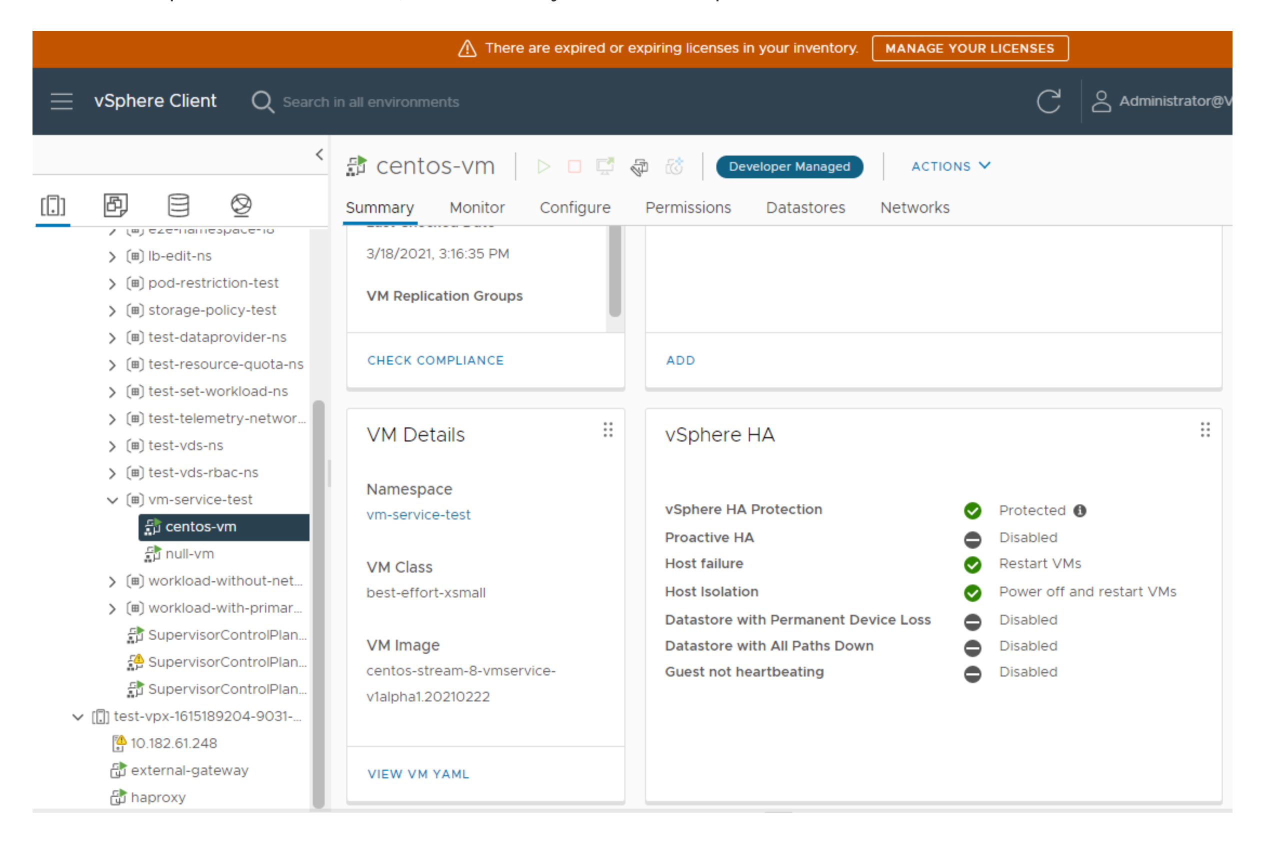
3 Seleccione la máquina virtual que desea ver y haga clic en la pestaña **Resumen**.

   Asegúrese de que ve la etiqueta **Administrado por el desarrollador** en la parte superior de la página **Resumen**.

   La página muestra información sobre la máquina virtual, incluidos el sistema operativo invitado y las direcciones IP.



4 Haga clic en **Cambiar a nueva vista** en la esquina superior derecha de la página para mostrar detalles adicionales, como la clase de máquina virtual y la imagen de la máquina virtual, así como el espacio de nombres, donde se ejecuta la máquina virtual.



Aprovisionar y operar clústeres TKGS

13

vSphere with Tanzu proporciona herramientas prácticas y flujos de trabajo sencillos para aprovisionar y operar clústeres de Tanzu Kubernetes. Consulte los procedimientos y ejemplos para crear y personalizar clústeres con varias configuraciones que se adapten a sus necesidades.

Este capítulo incluye los siguientes temas:

- Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS
- Clases de máquina virtual para clústeres de Tanzu Kubernetes
- Aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS
- Aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha1 de servicio Tanzu Kubernetes Grid
- Eliminar un clúster de Tanzu Kubernetes
- Especificar un editor de texto predeterminado para Kubectl
- Operar clústeres de Tanzu Kubernetes

Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS

Para aprovisionar clústeres de Tanzu Kubernetes, se debe invocar a la API declarativa de servicio Tanzu Kubernetes Grid mediante kubectl y una especificación de clúster definida en YAML. Después de aprovisionar un clúster, puede usarlo e implementar cargas de trabajo en él mediante kubectl.

Este flujo de trabajo es compatible con la API v1alpha2 de TKGS para aprovisionar clústeres de Tanzu Kubernetes de servicio Tanzu Kubernetes Grid. Si utiliza la Parámetros de configuración para clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1, consulte ese Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha1 de servicio Tanzu Kubernetes Grid.

Requisitos previos

Compruebe la finalización de los siguientes requisitos previos antes de iniciar el procedimiento de flujo de trabajo:

- Instale o actualice el entorno para admitir la API v1alpha2 de TKGS para aprovisionar clústeres de Tanzu Kubernetes de servicio Tanzu Kubernetes Grid. Consulte los Requisitos para usar la API v1alpha2 de TKGS para obtener más información. La versión de Tanzu Kubernetes mínima que admite la API v1alpha2 de TKGS para aprovisionar clústeres de Tanzu Kubernetes es `v1.21.2`. Consulte las notas de la versión de VMware Tanzu Kubernetes para obtener más información.
- Configure un espacio de nombres de vSphere para alojar clústeres de Tanzu Kubernetes. El espacio de nombres requiere permisos de edición para los ingenieros de desarrollo y operaciones y el almacenamiento compartido. Consulte Creación y configuración de un espacio de nombres de vSphere.
- Cree una biblioteca de contenido para versiones de Tanzu Kubernetes y sincronice las versiones que desea utilizar. Consulte Crear y administrar bibliotecas de contenido para versiones de Tanzu Kubernetes.
- Decida qué clases de máquinas virtuales predeterminadas desea utilizar y si necesita clases de máquina virtual personalizadas. Consulte Clases de máquina virtual para clústeres de Tanzu Kubernetes.
- Asocie la biblioteca de contenido y las clases de máquinas virtuales con el espacio de nombres de vSphere. Consulte Configurar un espacio de nombres de vSphere para las versiones de Tanzu Kubernetes.

Procedimiento

1. Descargue e instale las Herramientas de la CLI de Kubernetes para vSphere.

   Para obtener instrucciones, consulte Descargar e instalar Herramientas de la CLI de Kubernetes para vSphere.

2. Autentíquese con clúster supervisor mediante complemento de vSphere para kubectl.

   ```
   kubectl vsphere login --server=IP-ADDRESS --vsphere-username USERNAME
   ```

   Para obtener instrucciones, consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

3. Compruebe que el inicio de sesión en clúster supervisor se haya realizado correctamente.

   Debe aparecer un error similar al siguiente:

   ```
   Logged in successfully.

   You have access to the following contexts:
      192.197.2.65
      tkgs-ns
   ```

Donde `192.197.2.65` es el contexto de clúster supervisor y `tkgs-ns` es el contexto para el espacio de nombres de vSphere donde planea aprovisionar el clúster de Tanzu Kubernetes.

4 Compruebe que el destino espacio de nombres de vSphere sea el contexto actual.

```
kubectl config get-contexts
```

```
CURRENT   NAME            CLUSTER         AUTHINFO                              NAMESPACE
          192.197.2.65    192.197.2.65    wcp:192.197.2.65:user@vsphere.local
*         tkgs-ns         192.197.2.65    wcp:192.197.2.65:user@vsphere.local   tkgs-ns
```

Si el espacio de nombres de vSphere de destino no es el contexto actual, cambie a él.

```
kubectl config use-context tkgs-ns
```

5 Enumere los enlaces de clase de máquina virtual que están disponibles en el espacio de nombres de vSphere de destino.

```
kubectl get virtualmachineclassbindings
```

Solo puede utilizar las clases de máquina virtual que están enlazadas al espacio de nombres de destino. Si no ve ninguna clase de máquina virtual, compruebe que espacio de nombres de vSphere tenga las clases de máquina virtual predeterminadas agregadas.

6 Obtiene las clases de almacenamiento de volumen persistente disponibles.

```
kubectl describe storageclasses
```

7 Lista de versiones de Tanzu Kubernetes disponibles:

Puede utilizar cualquiera de los siguientes comandos para realizar esta operación:

```
kubectl get tkr
```

```
kubectl get tanzukubernetesreleases
```

Solo puede utilizar esas versiones que devuelve este comando. Si no ve ninguna versión o las versiones que desea, compruebe que haya sincronizado los archivos OVA deseados con la biblioteca de contenido.

8 Cree el archivo YAML para aprovisionar un clúster de Tanzu Kubernetes.

a Revise la especificación de la API v1alpha2 de TKGS para aprovisionar clústeres de Tanzu Kubernetes.

b Comience con uno de los YAML de ejemplo para el aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS para aprovisionar un clúster; ya sea Ejemplo de YAML para aprovisionar un clúster de Tanzu Kubernetes predeterminado o Ejemplo de YAML para aprovisionar un clúster de Tanzu Kubernetes personalizado según sus requisitos.

c Guarde el archivo YAML como `tkgs-cluster-1.yaml` o un formato similar.

d Rellene el archivo YAML en función de sus requisitos y utilice la información que obtuvo de los resultados de los comandos anteriores incluidos:

- El nombre del clúster, como `tkgs-cluster-1`
- El espacio de nombres de vSphere de destino, como `tkgs-ns`
- Clases de máquina virtual enlazadas, como `guaranteed-medium` y `guaranteed-small`
- Clases de almacenamiento para nodos de clúster y cargas de trabajo, como `vwt-storage-policy`
- El número de nodos de trabajo y plano de control (réplicas)
- La versión de Tanzu Kubernetes especificada por la cadena NAME de TKR, como `v1.21.6---vmware.1-tkg.1.b3d708a`

e Personalice el archivo YAML según sea necesario. Por ejemplo:

- Agregar volúmenes separados para componentes de renovación alta, como `etcd` y `containerd`
- Especificar una clase de almacenamiento persistente predeterminada para los nodos del clúster
- Personalizar las redes del clúster, incluidos los CIDR de CNI, pod y servicio

El resultado de este paso es un YAML válido para aprovisionar el clúster de TKGS. Por ejemplo:

```
apiVersion: run.tanzu.vmware.com/v1alpha2
kind: TanzuKubernetesCluster
metadata:
  name: tkgs-cluster-1
  namespace: tkgs-ns
spec:
  topology:
    controlPlane:
      replicas: 3
      vmClass: guaranteed-medium
      storageClass: vwt-storage-policy
      volumes:
        - name: etcd
          mountPath: /var/lib/etcd
          capacity:
            storage: 4Gi
      tkr:
        reference:
          name: v1.21.6---vmware.1-tkg.1.b3d708a
    nodePools:
    - name: worker-nodepool-a1
      replicas: 3
      vmClass: guaranteed-medium
      storageClass: vwt-storage-policy
```

```
      volumes:
        - name: containerd
          mountPath: /var/lib/containerd
          capacity:
            storage: 16Gi
      tkr:
        reference:
          name: v1.21.6---vmware.1-tkg.1.b3d708a
    - name: worker-nodepool-a2
      replicas: 2
      vmClass: guaranteed-small
      storageClass: vwt-storage-policy
      tkr:
        reference:
          name: v1.21.6---vmware.1-tkg.1.b3d708a
  settings:
    storage:
      defaultClass: vwt-storage-policy
```

Nota En el ejemplo anterior, se utilizan las redes de clúster predeterminadas, es decir, los rangos de CNI de Antrea y CIDR predeterminados para los servicios y los pods del clúster.

9 Ejecute el siguiente comando kubectl para aprovisionar el clúster.

```
kubectl apply -f tkgs-cluster-1.yaml
```

Resultado esperado:

```
tanzukubernetescluster.run.tanzu.vmware.com/tkgs-cluster-1 created
```

10 Supervise la implementación de nodos del clúster mediante kubectl.

```
kubectl get tanzukubernetesclusters
```

Inicialmente, el clúster no está listo porque se está aprovisionando.

```
NAME             CONTROL PLANE   WORKER   TKR NAME                           AGE
READY   TKR COMPATIBLE   UPDATES AVAILABLE
tkgs-cluster-1   3               5        v1.21.6---vmware.1-tkg.1.b3d708a   2m4s
False   True
```

Después de unos minutos, el estado READY debe ser True.

```
NAME             CONTROL PLANE   WORKER   TKR NAME                           AGE   READY
TKR COMPATIBLE   UPDATES AVAILABLE
tkgs-cluster-1   3               5        v1.21.6---vmware.1-tkg.1.b3d708a   13m   True
True
```

Para obtener más instrucciones, consulte Supervisar el estado del clúster de Tanzu Kubernetes mediante kubectl.

11 Supervise la implementación de nodos del clúster mediante vSphere Client.

En el inventario de **hosts y clústeres** de vSphere, debería ver los nodos de máquina virtual que se están implementando en el espacio de nombres de vSphere de destino.

Para obtener más instrucciones, consulte Supervisar el estado del clúster de Tanzu Kubernetes mediante vSphere Client.

12 Ejecute comandos `kubectl` adicionales para verificar el aprovisionamiento de los clústeres.

```
kubectl get tanzukubernetescluster,cluster-
api,virtualmachinesetresourcepolicy,virtualmachineservice,virtualmachine
```

Para obtener instrucciones adicionales, consulte Usar comandos operativos del clúster de Tanzu Kubernetes.

Para soluciones de problemas, consulte Solución de problemas de clústeres de Tanzu Kubernetes.

13 Con complemento de vSphere para kubectl, inicie sesión en el clúster.

```
kubectl vsphere login --server=IP-ADDRESS --vsphere-username USERNAME \
--tanzu-kubernetes-cluster-name CLUSTER-NAME \
--tanzu-kubernetes-cluster-namespace NAMESPACE-NAME
```

Por ejemplo:

```
kubectl vsphere login --server=192.197.2.65 --vsphere-username user@vsphere.local \
--tanzu-kubernetes-cluster-name tkgs-cluster-1 --tanzu-kubernetes-cluster-namespace tkgs-ns
```

Para obtener más instrucciones, consulte Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.

14 Compruebe que el inicio de sesión en el clúster de Tanzu Kubernetes sea correcto.

Debe aparecer un error similar al siguiente..

```
Logged in successfully.

You have access to the following contexts:
   192.197.2.65
   tkgs-cluster-1
   tkgs-ns
```

Donde `192.197.2.65` es el contexto de clúster supervisor, `tkgs-ns` es el contexto de espacio de nombres de vSphere y `tkgs-cluster-1` es el contexto del clúster de Tanzu Kubernetes.

15 Enumere los contextos de clúster disponibles mediante `kubectl`.

```
kubectl config get-contexts
```

Por ejemplo:

```
CURRENT   NAME             CLUSTER        AUTHINFO
NAMESPACE
          192.197.2.65     192.197.2.65   wcp:192.197.2.65:administrator@vsphere.local
*         tkgs-cluster-1   192.197.2.67   wcp:192.197.2.67:administrator@vsphere.local
          tkgs-ns          192.197.2.65   wcp:192.197.2.65:administrator@vsphere.local
tkgs-ns
```

Si es necesario, utilice `kubect config use-context tkgs-cluster-1` para cambiar al clúster de Tanzu Kubernetes para que sea el contexto actual.

16 Compruebe el aprovisionamiento de clústeres mediante los siguientes comandos de kubectl.

```
kubectl get nodes
```

Por ejemplo:

```
NAME                                                       STATUS   ROLES
AGE   VERSION
tkgs-cluster-1-control-plane-6ln2h                         Ready    control-plane,master
30m   v1.21.6+vmware.1
tkgs-cluster-1-control-plane-6q67n                         Ready    control-plane,master
33m   v1.21.6+vmware.1
tkgs-cluster-1-control-plane-jw964                         Ready    control-plane,master
37m   v1.21.6+vmware.1
tkgs-cluster-1-worker-nodepool-a1-4vvkb-65494d66d8-h5fp8   Ready    <none>
32m   v1.21.6+vmware.1
tkgs-cluster-1-worker-nodepool-a1-4vvkb-65494d66d8-q4g24   Ready    <none>
33m   v1.21.6+vmware.1
tkgs-cluster-1-worker-nodepool-a1-4vvkb-65494d66d8-vdcn4   Ready    <none>
33m   v1.21.6+vmware.1
tkgs-cluster-1-worker-nodepool-a2-2n22f-bd59d7b96-nh4dg    Ready    <none>
34m   v1.21.6+vmware.1
tkgs-cluster-1-worker-nodepool-a2-2n22f-bd59d7b96-vvfmf    Ready    <none>
33m   v1.21.6+vmware.1
```

17 Compruebe el aprovisionamiento de clústeres mediante los comandos de kubectl adicionales.

```
kubectl get namespaces
```

```
kubectl get pods -A
```

```
kubectl cluster-info
```

```
kubectl api-resources
```

18 Defina la directiva de seguridad de pods adecuada.

Los clústeres de Tanzu Kubernetes tienen el controlador de admisión de PodSecurityPolicy habilitado de forma predeterminada. Para obtener instrucciones, consulte Usar las directivas de seguridad de pods con clústeres de Tanzu Kubernetes.

Según la carga de trabajo y el usuario, deberá crear enlaces para un objeto PodSecurityPolicy suministrado por el sistema o crear un objeto PodSecurityPolicy personalizado. Consulte Ejemplo de enlaces de funciones para la directiva de seguridad de pods.

19 Implemente una carga de trabajo de ejemplo y compruebe la creación del clúster.

Para obtener instrucciones, consulte Implementar cargas de trabajo en clústeres de Tanzu Kubernetes.

20 Implemente extensiones de TKG para hacer que el clúster se implemente de forma operativa.

Para obtener instrucciones, consulte Implementar paquetes TKG en clústeres de Tanzu Kubernetes.

Clases de máquina virtual para clústeres de Tanzu Kubernetes

Para cambiar nodos del clúster de Tanzu Kubernetes, especifique la clase de máquina virtual. vSphere with Tanzu proporciona clases predeterminadas y puede crear las suyas propias. Para utilizar una clase, asóciela con la instancia de espacio de nombres de vSphere destino y haga referencia a la clase del manifiesto.

Acerca de las clases de máquinas virtuales

Una clase de máquina virtual es una solicitud de reservas de recursos para potencia de procesamiento en la máquina virtual (VM), incluidas la CPU y la memoria (RAM). Por ejemplo: el tipo de clase de máquina virtual denominado "guaranteed-large" reserva 4 CPU y 16 GB de RAM. Consulte Clases de máquinas virtuales predeterminadas para obtener una lista de las clases de máquinas virtuales predeterminadas y sus correspondientes reservas de CPU y RAM.

Nota El tamaño de disco de la máquina virtual se establece mediante la plantilla de OVA, no la definición de clase de máquina virtual. Para versiones de Tanzu Kubernetes, el tamaño de disco es de 16 GB. Consulte Acerca de las distribuciones de versión de Tanzu Kubernetes.

Existen dos tipos de reserva para las clases de máquina virtual: garantizada y mejor esfuerzo. La clase garantizada reserva por completo los recursos configurados. Esto significa que, para un clúster determinado, `spec.policies.resources.requests` coincide con la configuración de `spec.hardware`. La clase de mejor esfuerzo permite que se genere un compromiso excesivo de los recursos. Para las cargas de trabajo de producción se recomienda utilizar el tipo de clase de máquina virtual garantizada.

Advertencia Debido a que el tipo de clase de máquina virtual de mejor esfuerzo permite que los recursos se sobreasignen, puede quedarse sin recursos si estableció límites en el espacio de nombres de vSphere donde está aprovisionando el clúster de Tanzu Kubernetes. Si se produce una contención y el plano de control se ve afectado, el clúster puede dejar de ejecutarse. Por este motivo, siempre debe utilizar el tipo de clase de máquina virtual garantizada para los clústeres de producción. Si no puede usar el tipo de clase de máquina virtual garantizada para todos los nodos de producción, debe usarlo como mínimo para los nodos del plano de control.

Usar clases de máquinas virtuales

Para usar una clase de máquina virtual con un clúster de Tanzu Kubernetes, la clase de máquina virtual debe estar enlazada con el espacio de nombres de vSphere donde se aprovisiona el clúster. Para ello, asocie la clase con el espacio de nombres de destino. Consulte Configurar un espacio de nombres de vSphere para las versiones de Tanzu Kubernetes.

Para enumerar las clases de máquina virtual disponibles en el espacio de nombres de vSphere de destino, use el comando `kubectl get virtualmachineclassbinding`. Para ver todas las clases de máquinas virtuales presentes en el clúster supervisor, ejecute el comando `kubectl describe virtualmachineclasses`. Sin embargo, tenga en cuenta que, debido a que solo se pueden usar clases enlazadas para aprovisionar un clúster, este último comando es solo informativo. Consulte Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS.

Nota El requisito para asociar las clases de máquina virtual con el espacio de nombres de vSphere solo se aplica a clústeres nuevos. Los clústeres de Tanzu Kubernetes existentes que utilizan clases de máquina virtual predeterminadas siguen funcionando sin necesidad de asociación de espacio de nombres.

Clases de máquinas virtuales predeterminadas

La tabla Tabla 13-1. Clases de máquinas virtuales predeterminadas muestra los tipos de clase de máquina virtual predeterminados que se utilizan como tamaños de implementación de máquina virtual para los nodos del clúster de Tanzu Kubernetes.

Para evitar la sobreasignación de recursos, las cargas de trabajo de producción deben utilizar el tipo de clase garantizado. Para evitar quedarse sin memoria, no utilice el tamaño de clase pequeño o muy pequeño para ningún nodo de trabajo en el que implemente cargas de trabajo en cualquier entorno (desarrollo, prueba o producción).

Tabla 13-1. Clases de máquinas virtuales predeterminadas

Clase	CPU	Memoria (GB)	CPU y memoria reservadas
guaranteed-8xlarge	32	128	Sí
best-effort-8xlarge	32	128	No
guaranteed-4xlarge	16	128	Sí
best-effort-4xlarge	16	128	No
guaranteed-2xlarge	8	64	Sí
best-effort-2xlarge	8	64	No
guaranteed-xlarge	4	32	Sí
best-effort-xlarge	4	32	No
guaranteed-large	4	16	Sí
best-effort-large	4	16	No
guaranteed-medium	2	8	Sí
best-effort-medium	2	8	No
guaranteed-small	2	4	Sí
best-effort-small	2	4	No
guaranteed-xsmall	2	2	Sí
best-effort-xsmall	2	2	No

Clases de máquinas virtuales personalizadas

vSphere with Tanzu admite clases de máquinas virtuales personalizadas para usarlas con clústeres de Tanzu Kubernetes. Una vez que haya definido una clase de máquina virtual personalizada, debe asociarla con el espacio de nombres de vSphere de destino para poder utilizarla con un clúster. Consulte Crear una clase de máquina virtual en vSphere with Tanzu.

Editar clases de máquinas virtuales

Las definiciones de clase de máquina virtual no son inmutables. Todas las clases de máquina virtual se pueden Editar o eliminar una clase de máquina virtual en vSphere with Tanzu, incluidas las Clases de máquina virtual para clústeres de Tanzu Kubernetes. Si se edita una clase de máquina virtual, los nodos del clúster de Tanzu Kubernetes existentes no se ven afectados. Los clústeres de Tanzu Kubernetes nuevos utilizarán la definición de clase modificada.

Precaución Si edita una clase de máquina virtual que está utilizando un clúster de Tanzu Kubernetes y, a continuación, escala horizontalmente ese clúster, los nodos nuevos utilizarán la definición de clase editada, pero los nodos existentes usarán la definición de clase inicial, lo que provocará un error de coincidencia de clases.

Aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS

En esta sección, se describe cómo aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS.

Requisitos para usar la API v1alpha2 de TKGS

Para utilizar la API v1alpha2 de servicio Tanzu Kubernetes Grid para el aprovisionamiento de clústeres de Tanzu Kubernetes, cumpla con la lista completa de requisitos.

Requisitos para usar la API v1alpha2 de TKGS

La API v1alpha2 de servicio Tanzu Kubernetes Grid proporciona un conjunto sólido de mejoras para el aprovisionamiento de clústeres de Tanzu Kubernetes. Para obtener más información, consulte API v1alpha2 de TKGS para aprovisionar clústeres de Tanzu Kubernetes.

Para aprovechar la nueva funcionalidad que proporciona la API v1alpha2 de servicio Tanzu Kubernetes Grid, el entorno debe cumplir con cada uno de los siguientes requisitos.

Requisito	Referencia
Administración de cargas de trabajo está habilitada con redes compatibles, ya sea NSX-T Data Center o vSphere vDS nativa. **Nota** Una característica en particular puede requerir un tipo específico de redes. Si es así, se indica en el tema de esa función.	Consulte Requisitos previos para configurar vSphere with Tanzu en un clúster de vSphere. Consulte Habilitar la administración de cargas de trabajo con redes de NSX-T Data Center. Consulte Habilitar la administración de cargas de trabajo con redes de vSphere.
El vCenter Server que aloja **Administración de cargas de trabajo** se actualizó a la versión 7 Update 3 o una posterior.	Consulte las notas de la versión **Versiones de actualización y revisión de vCenter Server**. Para obtener instrucciones de actualización, consulte Actualizar vCenter Server Appliance.

Requisito	Referencia
Todos los hosts ESXi que admiten el clúster de vCenter Server en el que está habilitada **Administración de cargas de trabajo** se actualizan a la versión 7 Update 3 o una posterior.	Consulte las **notas de la versión de actualización y revisión de ESXi**. Para obtener instrucciones de actualización, consulte Actualizar hosts ESXi.
espacios de nombres de vSphere se actualiza a `v0.0.11` o una versión posterior.	Para obtener más información, consulte las notas de la versión de vSphere with Tanzu. Para obtener instrucciones de actualización, consulte Capítulo 17 Actualizar el entorno de vSphere with Tanzu.
clúster supervisor se actualiza a `v1.21.0+vmware.wcp.2` o una versión posterior.	Para obtener más información, consulte las notas de la versión de vSphere with Tanzu. Para obtener instrucciones de actualización, consulte Actualizar clúster supervisor mediante una actualización de los espacios de nombres de vSphere.

Requisito	Referencia
Debe utilizar Tanzu Kubernetes versión `v1.21.2---vmware.1-tkg.1.ee25d55` o una posterior.	Para obtener detalles de la versión, consulte Comprobar la compatibilidad del clúster de Tanzu Kubernetes para actualizar. Para obtener instrucciones sobre cómo aprovisionar clústeres nuevos, consulte YAML de ejemplo para el aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS. Para obtener instrucciones sobre cómo actualizar un clúster existente, consulte Actualizar una versión de Tanzu Kubernetes después de convertir la especificación del clúster a la API v1alpha2 de TKGS.
Consideraciones de CNI para los límites de nodos	El valor predeterminado de la configuración de la especificación del clúster `spec.settings.network.pods.cidrBlocks` es 192.168.0.0/16. Consulte API v1alpha2 de TKGS para aprovisionar clústeres de Tanzu Kubernetes. Si personaliza, el tamaño mínimo del bloque CIDR de los pods es /24. Sin embargo; tenga cuidado al restringir la máscara de subred de `pods.cidrBlocks` más allá de /16. TKGS asigna a cada nodo de clúster una subred /24 creada desde `pods.cidrBlocks`. Esta asignación se determina mediante el parámetro Administrador de controladoras de Kubernetes > NodeIPAMController denominado NodeCIDRMaskSize que establece el tamaño de la máscara de subred para el CIDR de nodo en el clúster. La máscara de subred del nodo predeterminada es /24 para IPv4. Debido a que cada nodo de un clúster obtiene una subred /24 de `pods.cidrBlocks`, puede quedarse sin direcciones IP de nodo si utiliza un tamaño de máscara de subred que sea demasiado restrictivo para el clúster que está aprovisionando. Los siguientes límites de nodos se aplican a un clúster de Tanzu Kubernetes aprovisionado con la CNI de Antrea o Calico. /16 == 150 nodos máx. (por ConfigMax) /17 == 128 nodos máx. /18 == 64 nodos como máximo /19 == 32 nodos como máximo /20 == 16 nodos como máximo /21 == 8 nodos como máximo /22 == 4 nodos como máximo /23 == 2 nodos como máximo /24 == 1 nodo máx.

API v1alpha2 de TKGS para aprovisionar clústeres de Tanzu Kubernetes

La API v1alpha2 de servicio Tanzu Kubernetes Grid permite aprovisionar clústeres de Tanzu Kubernetes de forma declarativa. Consulte la lista y la descripción de todos los parámetros, y las directrices de uso para crear y personalizar los clústeres.

Especificación de la API v1alpha2 de servicio Tanzu Kubernetes Grid para aprovisionar clústeres de Tanzu Kubernetes

La especificación de YAML enumera todos los parámetros disponibles para aprovisionar un clúster de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha2.

```
apiVersion: run.tanzu.vmware.com/v1alpha2
kind: TanzuKubernetesCluster
metadata:
  name: string
  namespace: string
spec:
  topology:
    controlPlane:
      replicas: int32
      vmClass: string
      storageClass: string
      volumes:
        - name: string
          mountPath: string
          capacity:
            storage: size in GiB
      tkr:
        reference:
          name: string
      nodeDrainTimeout: string
    nodePools:
    - name: string
      labels: map[string]string
      taints:
        -  key: string
           value: string
           effect: string
           timeAdded: time
      replicas: int32
      vmClass: string
      storageClass: string
      volumes:
        - name: string
          mountPath: string
          capacity:
            storage: size in GiB
      tkr:
        reference:
          name: string
      nodeDrainTimeout: string
  settings:
```

```
    storage:
      classes: [string]
      defaultClass: string
    network:
      cni:
        name: string
      pods:
        cidrBlocks: [string]
      services:
        cidrBlocks: [string]
      serviceDomain: string
      proxy:
        httpProxy: string
        httpsProxy: string
        noProxy: [string]
      trust:
        additionalTrustedCAs:
          - name: string
            data: string
```

Especificación de la API v1alpha2 de servicio Tanzu Kubernetes Grid anotada para aprovisionar los clústeres de Tanzu Kubernetes

La especificación de YAML anotada enumera todos los parámetros disponibles para aprovisionar un clúster de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha2 con la documentación de cada campo.

Nota Actualmente, todos los campos `tkr.reference.name` deben coincidir. En el futuro, es posible que se admitan diferentes versiones de Tanzu Kubernetes para los grupos de nodos.

```
apiVersion: run.tanzu.vmware.com/v1alpha2
kind: TanzuKubernetesCluster
#metadata defines cluster information
metadata:
  #name for this Tanzu Kubernetes cluster
  name: string
  #namespace vSphere Namespace where to provision this cluster
  namespace: string
#spec defines cluster configuration
spec:
  #topology describes the number, purpose, organization
  #of nodes and the resources allocated for each
  #nodes are grouped into pools based on their purpose
  #`controlPlane` is special kind of a node pool
  #`nodePools` is for groups of worker nodes
  #each node pool is homogeneous: its nodes have the same
  #resource allocation and use the same storage
  topology:
    #controlPlane defines the topology of the cluster
    #controller, including the number of nodes and
    #the resources allocated for each
    #control plane must have an odd number of nodes
    controlPlane:
```

```
      #replicas is the number of nodes in the pool
      #the control plane can have 1 or 3 nodes
      #defaults to 1 if `nil`
      replicas: int32
      #vmClass is the name of the VirtualMachineClass
      #which describes the virtual hardware settings
      #to be used for each node in the node pool
      #vmClass controls the CPU and memory available
      #to the node and the requests and limits on
      #those resources; to list available vm classes run
      #`kubectl describe virtualmachineclasses`
      vmClass: string
      #storageClass to be used for storage of the disks
      #which store the root filesystems of the nodes
      #to list available storage classes run
      #`kubectl describe storageclasses`
      storageClass: string
      #volumes is the optional set of PVCs to create
      #and attach to each node; use for high-churn
      #control plane components such as etcd
      volumes:
        #name of the PVC to be used as the suffix (node.name)
        - name: string
          #mountPath is the directory where the volume
          #device is mounted; takes the form /dir/path
          mountPath: string
          #capacity is the PVC capacity
          capacity:
            #storage to be used for the disk
            #volume; if not specified defaults to
            #`spec.controlPlane.storageClass`
            storage: size in GiB
      #tkr.reference.name is the TKR NAME
      #to be used by control plane nodes; supported
      #format is `v1.21.2---vmware.1-tkg.1.ee25d55`
      #currently all `tkr.reference.name` fields must match
      tkr:
        reference:
          name: string
      #nodeDrainTimeout is the total amount of time
      #the controller will spend draining a node
      #the default value is 0 which means the node is
      #drained without any time limit
      nodeDrainTimeout: string
    #nodePools is an array that describes a group of
    #worker nodes in the cluster with the same configuration
    nodePools:
    #name of the worker node pool
    #must be unique in the cluster
    - name: string
      #labels are an optional map of string keys and values
      #to organize and categorize objects
      #propagated to the created nodes
      labels: map[string]string
      #taints specifies optional taints to register the
```

```
      #Node API object with; user-defined taints are
      #propagated to the created nodes
      taints:
        #key is the taint key to be applied to a node
        -  key: string
        #value is the taint value corresponding to the key
           value: string
        #effect is the effect of the taint on pods
        #that do not tolerate the taint; valid effects are
        #`NoSchedule`, `PreferNoSchedule`, `NoExecute`
           effect: string
        #timeAdded is the time when the taint was added
        #only written by the system for `NoExecute` taints
           timeAdded: time
      #replicas is the number of nodes in the pool
      #worker nodePool can have from 0 to 150 nodes
      #value of `nil` means the field is not reconciled,
      #allowing external services like autoscalers
      #to choose the number of nodes for the nodePool
      #by default CAPI's `MachineDeployment` will pick 1
      #NOTE: a cluster provisioned with 0 worker nodes/nodepools
      #is not assigned any load balancer services
      replicas: int32
      #vmClass is the name of the VirtualMachineClass
      #which describes the virtual hardware settings
      #to be used for each node in the pool
      #vmClass controls the CPU and memory available
      #to the node and the requests and limits on
      #those resources; to list available vm classes run
      #`kubectl describe virtualmachineclasses`
      vmClass: string
      #storageClass to be used for storage of the disks
      #which store the root filesystems of the nodes
      #to list available storage classes run
      #`kubectl describe ns`
      storageClass: string
      #volumes is the optional set of PVCs to create
      #and attach to each node for high-churn worker node
      #components such as the container runtime
      volumes:
        #name of this PVC to be used as the suffix (node.name)
        - name: string
          #mountPath is the directory where the volume
          #device is mounted; takes the form /dir/path
          mountPath: string
          #capacity is the PVC capacity
          capacity:
            #storage to be used for the disk
            #volume; if not specified defaults to
            #`topology.nodePools[*].storageClass`
            storage: size in GiB
      #tkr.reference.name points to the TKR NAME
      #to be used by `spec.topology.nodePools[*]` nodes; supported
      #format is `v1.21.2---vmware.1-tkg.1.ee25d55`
      #currently all `tkr.reference.name` fields must match
```

```
    tkr:
      reference:
        name: string
    #nodeDrainTimeout is the total amount of time
    #the controller will spend draining a node
    #the default value is 0 which means the node is
    #drained without any time limit
    nodeDrainTimeout: string
#settings are optional runtime configurations
#for the cluster, including persistent storage
#for pods and node network customizations
settings:
  #storage defines persistent volume (PV) storage entries
  #for container workloads; note that the storage used for
  #node disks is defined by `topology.controlPlane.storageClass`
  #and by `spec.topology.nodePools[*].storageClass`
  storage:
    #classes is a list of persistent volume (PV) storage
    #classes to expose for container workloads on the cluster
    #any class specified must be associated with the
    #vSphere Namespace where the cluster is provisioned
    #if omitted, all storage classes associated with the
    #namespace will be exposed in the cluster
    classes: [string]
    #defaultClass treats the named storage class as the default
    #for the cluster; because all namespaced storage classes
    #are exposed if specific `classes` are not named,
    #classes is not required to specify a defaultClass
    #many workloads, including TKG Extensions and Helm,
    #require a default storage class
    #if omitted, no default storage class is set
    defaultClass: string
  #netowrk defines custom networking for cluster workloads
  network:
    #cni identifies the CNI plugin for the cluster
    #use to override the default CNI set in the
    #tkgservicesonfiguration spec, or when customizing
    #network settings for the default CNI
    cni:
      #name is the name of the CNI plugin to use; supported
      #values are `antrea`, `calico`, `antrea-nsx-routed`
      name: string
    #pods configures custom networks for pods
    #defaults to 192.168.0.0/16 if CNI is `antrea` or `calico`
    #defaults to empty if CNI is `antrea-nsx-routed`
    #custom subnet size must equal or exceed /24
    #use caution before seeting CIDR range other than /16
    #cannot overlap with Supervisor Cluster workload network
    pods:
      #cidrBlocks is an array of network ranges; supplying
      #multiple ranges may not be supported by all CNI plugins
      cidrBlocks: [string]
    #services configures custom network for services
    #defaults to 10.96.0.0/12
    #cannot overlap with Supervisor Cluster workload network
```

```
    services:
      #cidrBlocks is an array of network ranges; supplying
      #multiple ranges many not be supported by all CNI plugins
      cidrBlocks: [string]
    #serviceDomain specifies the service domain for the cluster
    #defaults to `cluster.local`
    serviceDomain: string
    #proxy configures proxy server to be used inside the cluster
    #if omitted no proxy is configured
    proxy:
      #httpProxy is the proxy URI for HTTP connections
      #to endpoints outside the cluster
      #takes form `http://<user>:<pwd>@<ip>:<port>`
      httpProxy: string
      #httpsProxy is the proxy URL for HTTPS connections
      #to endpoints outside the cluster
      #takes the frorm `http://<user>:<pwd>@<ip>:<port>`
      httpsProxy: string
      #noProxy is the list of destination domain names, domains,
      #IP addresses, and other network CIDRs to exclude from proxying
      #must include Supervisor Cluster Pod, Egress, Ingress CIDRs
      noProxy: [string]
    #trust configures additional certificates for the cluster
    #if omitted no additional certificate is configured
    trust:
      #additionalTrustedCAs are additional trusted certificates
      #can be additional CAs or end certificates
      additionalTrustedCAs:
        #name is the name of the additional trusted certificate
        #must match the name used in the filename
        - name: string
          #data holds the contents of the additional trusted cert
          #PEM Public Certificate data encoded as base64 string
          #such as `LS0tLS1C...LS0tCg==` where "..." is the
          #middle section of the long base64 string
          data: string
```

YAML de ejemplo para el aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS

La API de TKGS proporciona valores predeterminados inteligentes y una gama de opciones para personalizar clústeres de Tanzu Kubernetes. Consulte los ejemplos para aprovisionar clústeres de varios tipos con configuraciones y personalizaciones diferentes para satisfacer sus necesidades.

Ejemplo de YAML para aprovisionar un clúster de Tanzu Kubernetes predeterminado

El siguiente ejemplo de YAML aprovisiona un clúster de Tanzu Kubernetes predeterminado mediante la API v1alpha2 de TKGS para aprovisionar clústeres de Tanzu Kubernetes. Este YAML de ejemplo utiliza todos los valores predeterminados disponibles y representa la configuración mínima necesaria para aprovisionar un clúster.

```
apiVersion: run.tanzu.vmware.com/v1alpha2
kind: TanzuKubernetesCluster
metadata:
  name: tkgs-v2-cluster-default
  namespace: tkgs-cluster-ns
spec:
  topology:
    controlPlane:
      replicas: 3
      vmClass: guaranteed-medium
      storageClass: vwt-storage-policy
      tkr:
        reference:
          name: v1.21.2---vmware.1-tkg.1.ee25d55
    nodePools:
    - name: worker-nodepool-a1
      replicas: 3
      vmClass: guaranteed-large
      storageClass: vwt-storage-policy
      tkr:
        reference:
          name: v1.21.2---vmware.1-tkg.1.ee25d55
```

Ejemplo de YAML para aprovisionar un clúster de Tanzu Kubernetes personalizado

El siguiente ejemplo de YAML aprovisiona un clúster de Tanzu Kubernetes personalizado mediante la API v1alpha2 de TKGS para aprovisionar clústeres de Tanzu Kubernetes de servicio Tanzu Kubernetes Grid. Este YAML de ejemplo especifica volúmenes independientes para los componentes de nodo de renovación alta y personaliza ciertas configuraciones de red y almacenamiento.

```
apiVersion: run.tanzu.vmware.com/v1alpha2
kind: TanzuKubernetesCluster
metadata:
  name: tkgs-v2-cluster-custom
  namespace: tkgs-cluster-ns
spec:
  topology:
    controlPlane:
      replicas: 3
      vmClass: guaranteed-medium
      storageClass: vwt-storage-policy
      volumes:
        - name: etcd
```

```
          mountPath: /var/lib/etcd
          capacity:
            storage: 4Gi
      tkr:
        reference:
          name: v1.21.2---vmware.1-tkg.1.ee25d55
    nodePools:
    - name: worker-nodepool-a1
      replicas: 3
      vmClass: guaranteed-large
      storageClass: vwt-storage-policy
      volumes:
        - name: containerd
          mountPath: /var/lib/containerd
          capacity:
            storage: 16Gi
      tkr:
        reference:
          name: v1.21.2---vmware.1-tkg.1.ee25d55
    - name: worker-nodepool-a2
      replicas: 2
      vmClass: guaranteed-medium
      storageClass: vwt-storage-policy
      tkr:
        reference:
          name: v1.21.2---vmware.1-tkg.1.ee25d55
    - name: worker-nodepool-a3
      replicas: 1
      vmClass: guaranteed-small
      storageClass: vwt-storage-policy
      tkr:
        reference:
          name: v1.21.2---vmware.1-tkg.1.ee25d55
  settings:
    storage:
      defaultClass: vwt-storage-policy
    network:
      cni:
        name: antrea
      services:
        cidrBlocks: ["198.53.100.0/16"]
      pods:
        cidrBlocks: ["192.0.5.0/16"]
      serviceDomain: cluster.local
      proxy:
        httpProxy: http://<user>:<pwd>@<ip>:<port>
        httpsProxy: http://<user>:<pwd>@<ip>:<port>
        noProxy: [10.246.0.0/16,192.168.144.0/20,192.168.128.0/20]
      trust:
        additionalTrustedCAs:
          - name: CompanyInternalCA-1
            data: LS0tLS1C...LS0tCg==
          - name: CompanyInternalCA-2
            data: MTLtMT1C...MT0tPg==
```

Actualizar una versión de Tanzu Kubernetes después de convertir la especificación del clúster a la API v1alpha2 de TKGS

Después de convertir automáticamente una especificación de clúster de Tanzu Kubernetes al formato de API v1alpha2, para realizar una actualización gradual del clúster de Tanzu Kubernetes, que normalmente se realiza cambiando la versión de Tanzu Kubernetes, es posible que deba realizar algún procesamiento previo de la especificación del clúster para evitar errores.

Conversión automática de especificaciones de clústeres

Para actualizar el entorno de vSphere with Tanzu a la API v1alpha2 de servicio Tanzu Kubernetes Grid, actualice el clúster supervisor donde se ejecuta el servicio.

Una vez que servicio Tanzu Kubernetes Grid ejecuta la API v1alpha2, el sistema convierte automáticamente todas las especificaciones del clúster de Tanzu Kubernetes existentes del formato v1alpha1 al formato v1alpha2. Durante el proceso de conversión automática, el sistema crea y rellena los campos esperados para cada manifiesto del clúster. Desusos y adiciones de la API enumera los campos de especificación del clúster que son nuevos y obsoletos en la API v1alpha2.

Para actualizar la versión de Tanzu Kubernetes para un clúster cuyo manifiesto se ha convertido automáticamente al formato v1alpha2, debe realizar un procesamiento previo manual para evitar errores. Ejemplos de actualización del clúster enumera varias opciones.

Desusos y adiciones de la API

En la tabla se enumeran los ajustes de especificación del clúster que están obsoletos en la API v1alpha2 y que se reemplazan por una nueva configuración.

Configuración obsoleta	Nueva configuración	Comentarios
`spec.distribution.version` `spec.distribution.fullVersion`	`spec.topology.controlPlane.tkr.refernece.name` `spec.topology.nodePools[*].tkr.reference.name`	Debe utilizar el formato TKR NAME. Consulte los ejemplos.
`spec.topology.workers`	`spec.topology.nodePools[*]`	En un clúster convertido, el bloque `spec.topology.workers` se convierte en `spec.topology.nodePools[0]`. La primera entrada de la lista de `nodePools` es `name: workers`.
`spec.topology.controlPlane.count` `spec.topology.workers.count`	`spec.topology.controlPlane.replicas` `spec.topology.nodePools[*].replicas`	`count` se reemplaza con `replicas`
`spec.topology.controlPlane.class` `spec.topology.workers.class`	`spec.topology.controlPlane.vmClass` `spec.topology.nodePools[*].vmClass`	`class` se reemplaza con `vmClass`

Configuración obsoleta	Nueva configuración	Comentarios
N/C	spec.topology.nodePools[*].labels	Valores de par de claves opcionales para organizar y categorizar objetos; las etiquetas se propagan a los nodos creados
N/C	spec.topology.nodePools[*].taints	Manchas opcionales para registrar los nodos; las manchas definidas por el usuario se propagan a los nodos creados

Se requiere el formato TKR NAME

Además de que los campos `spec.distribution.version` están obsoletos, no se admite el formato DISTRIBUTION para especificar la versión de Tanzu Kubernetes. Esto significa que no se pueden utilizar los siguientes formatos de cadena para hacer referencia a la versión de destino: `1.21.2+vmware.1-tkg.1.ee25d55`, `1.21.2` y `1.21`.

Al hacer referencia a la versión de Tanzu Kubernetes en una especificación de clúster de API v1alpha2, debe utilizar el formato TKR NAME, no el formato obsoleto DISTRIBUTION. A pesar de que el formato obsoleto se muestra en la columna ACTUALIZACIONES DISPONIBLES, el único formato admitido es el que aparece en la columna TKR NAME.

```
kubectl get tanzukubernetescluster
NAMESPACE         NAME            CONTROL PLANE   WORKER   TKR
NAME                              AGE     READY   TKR COMPATIBLE   UPDATES AVAILABLE
tkgs-cluster-1   test-cluster    3               3        v1.21.2---vmware.1-
tkg.1.ee25d55     38h     True     True             [1.21.2+vmware.1-tkg.1.ee25d55]
```

Usar kubectl edit para actualizar una especificación de clúster

Si necesita realizar modificaciones en una especificación de clúster para que cumpla con la API v1alpha2 de TKGS, utilice el método `kubectl edit`. No intente utilizar el método `kubectl patch` para este tipo de actualización. Consulte Métodos para editar el manifiesto del clúster. Para configurar `kubectl` con un editor, consulte Especificar un editor de texto predeterminado para Kubectl.

Ejemplos de actualización del clúster

Debido a que cambiar `spec.distribution.version` es la forma más común de activar una actualización gradual del clúster (consulte Actualizar clústeres de Tanzu Kubernetes), y este campo está obsoleto en la API v1alpha2, existen algunas consideraciones que se deben tener en cuenta y algunas recomendaciones de procesamiento previo que se deben seguir para evitar posibles problemas de actualización del clúster.

Los siguientes ejemplos demuestran cómo actualizar la versión de un clúster de Tanzu Kubernetes que se aprovisionó mediante la API v1alpha1 a un sistema que ejecuta la API v1alpha2.

Ejemplo de actualización de clúster 1: Usar una sola referencia de TKR NAME en el plano de control

El enfoque recomendado es eliminar todos los bloques `nodePools[*].tkr.reference.name` de la especificación convertida y actualizar `controlPlane.tkr.reference.name` con el TKR NAME de la versión de destino. En este caso, la misma versión de Tanzu Kubernetes se propaga a todos los nodos `nodePools[*]`.

En el futuro, las versiones de Tanzu Kubernetes pueden ser diferentes entre `controlPlane` y `nodePools[*]`. Actualmente, sin embargo, todas las versiones de un clúster deben coincidir, por lo que basta con colocar una sola referencia de TKR NAME en `controlPlane`.

Por ejemplo:

```
apiVersion: run.tanzu.vmware.com/v1alpha2
kind: TanzuKubernetesCluster
metadata:
  name: tkgs-cluster-update-example1
  namespace: tkgs-cluster-ns
spec:
  settings:
    network:
      cni:
        name: antrea
      pods:
        cidrBlocks:
        - 192.0.2.0/16
      serviceDomain: cluster.local
      services:
        cidrBlocks:
        - 198.51.100.0/12
  topology:
    controlPlane:
      replicas: 3
      storageClass: vwt-storage-policy
      tkr:
        reference:
          name: v1.21.2---vmware.1-tkg.1.ee25d55
      vmClass: best-effort-medium
    nodePools:
    - name: workers
      replicas: 3
      storageClass: vwt-storage-policy
      vmClass: best-effort-medium
```

Ejemplo de actualización de clúster 2: Usar una referencia de TKR NAME para cada grupo de nodos

El segundo ejemplo es colocar TKR NAME en el bloque `tkr.reference.name` para las topologías `controlPlane` y `nodePools[*]`.

Este enfoque tiene la ventaja de estar listo para futuras versiones cuando la versión de Tanzu Kubernetes puede ser diferente en todos los grupos de nodos. Actualmente, deben coincidir.

Por ejemplo:

```
apiVersion: run.tanzu.vmware.com/v1alpha2
kind: TanzuKubernetesCluster
metadata:
  name: tkgs-cluster-update-example2
  namespace: tkgs-cluster-ns
spec:
  settings:
    network:
      cni:
        name: antrea
      pods:
        cidrBlocks:
        - 192.0.2.0/16
      serviceDomain: cluster.local
      services:
        cidrBlocks:
        - 198.51.100.0/12
  topology:
    controlPlane:
      replicas: 3
      storageClass: vwt-storage-policy
      vmClass: best-effort-medium
      tkr:
        reference:
          name: v1.21.2---vmware.1-tkg.1.ee25d55
    nodePools:
    - name: workers
      replicas: 3
      storageClass: vwt-storage-policy
      vmClass: best-effort-medium
      tkr:
        reference:
          name: v1.21.2---vmware.1-tkg.1.ee25d55
```

Ejemplo de actualización de clúster 3: Usar campos de distribución obsoletos

La opción final es utilizar los campos obsoletos `spec.distribution.fullVersion` y `spec.distribution.version`, y eliminar manualmente todos los bloques `tkr.reference.name`. Debe incluir ambos campos con uno con el formato TKR NAME y el otro anulado. No se admiten accesos directos de versiones como `v1.21.2` y `v1.21`.

Nota Para la versión de Tanzu Kubernetes en Ubuntu, no se admite el uso de `spec.distribution.version`.

En el siguiente ejemplo, se utiliza `fullVersion` con TKR NAME y un valor nulo (vacío) en el campo `version`. Se eliminan todas las entradas `tkr.reference.name`.

```
apiVersion: run.tanzu.vmware.com/v1alpha2
kind: TanzuKubernetesCluster
metadata:
  name: tkgs-cluster-update-example3a
  namespace: tkgs-cluster-ns
spec:
  distribution:
    fullVersion: v1.21.2---vmware.1-tkg.1.ee25d55
    version: ""
  settings:
    network:
      cni:
        name: antrea
      pods:
        cidrBlocks:
        - 192.0.2.0/16
      serviceDomain: cluster.local
      services:
        cidrBlocks:
        - 198.51.100.0/12
  topology:
    controlPlane:
      replicas: 3
      storageClass: vwt-storage-policy
      vmClass: best-effort-medium
    nodePools:
    - name: workers
      replicas: 3
      storageClass: vwt-storage-policy
      vmClass: best-effort-medium
```

Como alternativa, puede utilizar el campo `version` con TKR NAME y un valor nulo (vacío) en el campo `fullVersion`. Aunque esté utilizando el campo `version`, no se admiten accesos directos de versiones. Se eliminan todas las entradas `tkr.reference.name`.

```
apiVersion: run.tanzu.vmware.com/v1alpha2
kind: TanzuKubernetesCluster
metadata:
  name: tkgs-cluster-update-example3b
  namespace: tkgs-cluster-ns
spec:
  distribution:
    fullVersion: ""
    version: v1.21.2---vmware.1-tkg.1.ee25d55
  settings:
    network:
      cni:
        name: antrea
      pods:
        cidrBlocks:
        - 192.0.2.0/16
```

```
      serviceDomain: cluster.local
      services:
        cidrBlocks:
        - 198.51.100.0/12
  topology:
    controlPlane:
      replicas: 3
      storageClass: vwt-storage-policy
      vmClass: best-effort-medium
    nodePools:
    - name: workers
      replicas: 3
      storageClass: vwt-storage-policy
      vmClass: best-effort-medium
```

Configurar un clúster de Tanzu Kubernetes con una red de pods enrutable mediante la API v1alpha2

Puede configurar un clúster de Tanzu Kubernetes para utilizar redes de pods enrutables especificando `antrea-nsx-routed` como la CNI del clúster.

Introducción a las redes de pods enrutables

El Modelo de red de Kubernetes requiere que un pod de la red de nodos de un clúster pueda comunicarse con todos los pods de todos los nodos del mismo clúster sin traducción de direcciones de red (Network Address Translation, NAT). Para satisfacer este requisito, a cada pod de Kubernetes se le asigna una dirección IP que se asigna desde una red de pods dedicada.

Cuando se aprovisiona un clúster de Tanzu Kubernetes mediante los complementos de CNI `antrea` o `calico`, el sistema crea la red de pods predeterminada `192.168.0.0/16`. Esta subred es un espacio de direcciones privadas que solo es único dentro del clúster y no se puede enrutar en Internet. Aunque puede personalizar `network.pods.cidrBlocks`, la red de pods no se puede enrutar mediante estos complementos de CNI. Para obtener más información, consulte API v1alpha2 de TKGS para aprovisionar clústeres de Tanzu Kubernetes.

La API de servicio Tanzu Kubernetes Grid v1alpha2 admite redes de pods enrutables mediante el complemento de CNI de `antrea-nsx-routed`. Esta interfaz de red es un complemento de Antrea personalizado configurado para admitir redes de pods enrutables para clústeres de Tanzu Kubernetes. En la especificación de clúster, el campo de bloques CIDR de pods debe ser explícitamente nulo para que la administración de direcciones IP (IPAM) se controle mediante clúster supervisor.

Habilitar redes de pods enrutables permite que los pods se direccionen directamente desde un cliente externo al clúster. Además, las direcciones IP de los pods se conservan para que los servidores y los servicios de red externos puedan identificar los pods de origen y aplicar directivas basadas en direcciones IP. Patrones de tráfico compatibles, incluidos los siguientes:

- Se permite el tráfico entre un pod de clúster Tanzu Kubernetes y un pod de vSphere en el mismo espacio de nombres de vSphere.

- El tráfico se descarta entre un pod de clúster de Tanzu Kubernetes y un pod de vSphere en diferentes espacios de nombres de vSphere.
- Los nodos del plano de control de clúster supervisor pueden acceder a los pods del clúster de Tanzu Kubernetes.
- Los pods de clúster de Tanzu Kubernetes pueden alcanzar la red externa.
- La red externa no puede acceder a los pods de clúster de Tanzu Kubernetes. Las reglas de aislamiento de firewall distribuido (DFW) descartan el tráfico en los nodos del clúster de Tanzu Kubernetes.

Requisitos del sistema para pods enrutables

Las redes de pods enrutables requieren que clúster supervisor se configure con NSX-T Data Center. No se pueden utilizar pods enrutables con redes de vSphere vDS nativas.

Los pods enrutables requieren la API de servicio Tanzu Kubernetes Grid v1alpha2. Consulte Requisitos para usar la API v1alpha2 de TKGS.

Requisitos de configuración de NSX-T para pods enrutables

Además de los requisitos básicos, no se requiere una configuración especial de NSX-T para usar redes de pods enrutables con clústeres de Tanzu Kubernetes. Un entorno de vSphere with Tanzu que ejecuta vSphere U3 con NSX-T incluye la versión de NCP para admitir redes de pods enrutables. No se necesita ninguna configuración adicional de NSX-T.

NCP crea un grupo de direcciones IP para la red de pods enrutables desde uno de estos dos orígenes:

- Si la red de carga de trabajo está configurada con una red de espacio de nombres, NCP creará uno o más grupos de IP a partir de los bloques de IP especificados para esta red de espacio de nombres.
- Si no hay ninguna red de espacio de nombres especificada para la red de carga de trabajo, NCP creará uno o más grupos de direcciones IP desde el CIDR del pod de clúster supervisor.

Para obtener más información, consulte Agregar redes de cargas de trabajo a un clúster supervisor configurada con redes de VDS y Cambiar la configuración de red de carga de trabajo en un clúster supervisor configurada con NSX-T Data Center.

clúster supervisor Requisitos de configuración para pods enrutables

Además de los requisitos básicos, no se requiere ninguna configuración de clúster supervisor especial para usar redes de pods enrutables con clústeres de Tanzu Kubernetes.

Si las redes de pods enrutables están habilitadas como se describe a continuación, el CIDR de pods de clúster de Tanzu Kubernetes se asigna desde el grupo de direcciones IP creado desde la red de espacio de nombres o, si no hay ninguno, desde el CIDR de pods de clúster supervisor.

Debe asegurarse de que el CIDR de servicios de clúster supervisor que asigna las direcciones IP para los nodos del clúster no se superponga con el CIDR de la red de espacio de nombres o con el CIDR del pod de clúster supervisor.

Ejemplo de configuración de clúster para pods enrutables

El siguiente ejemplo de YAML muestra cómo configurar un clúster con una red de pods enrutable. es una configuración personalizada para invocar a servicio Tanzu Kubernetes Grid y aprovisionar un clúster de Tanzu Kubernetes mediante la API v1alpha2.

La especificación del clúster declara `antrea-nsx-routed` como la CNI para habilitar las redes de pods enrutables. Cuando se especifica la CNI es `antrea-nsx-routed`, el campo `pods.cidrBlock` debe estar vacío. Si se especifica `antrea-nsx-routed`, se producirá un error en el aprovisionamiento del clúster si no se utilizan redes de NSX-T.

```
apiVersion: run.tanzu.vmware.com/v1alpha2
kind: TanzuKubernetesCluster
metadata:
  name: tkgs-v2-cluster-routable-pods
  namespace: tkgs-cluster-ns
spec:
  topology:
    controlPlane:
      replicas: 3
      vmClass: guaranteed-medium
      storageClass: vwt-storage-policy
      tkr:
        reference:
          name: v1.21.2---vmware.1-tkg.1.ee25d55
    nodePools:
    - name: worker-nodepool-a1
      replicas: 3
      vmClass: guaranteed-large
      storageClass: vwt-storage-policy
      tkr:
        reference:
          name: v1.21.2---vmware.1-tkg.1.ee25d55
  settings:
    storage:
      defaultClass: vwt-storage-policy
    network:
      #`antrea-nsx-routed` is the required CNI
      #for routable pods
      cni:
        name: antrea-nsx-routed
      services:
        cidrBlocks: ["10.97.0.0/24"]
      serviceDomain: tanzukubernetescluster.local
      #`pods.cidrBlocks` value must be empty
      #when `antrea-nsx-routed` is the CNI
      pods:
        cidrBlocks:
```

Parámetros de configuración para la API v1alpha2 de TKGS

Puede personalizar servicio Tanzu Kubernetes Grid con ajustes globales de funciones clave, como la interfaz de redes de contenedor (Container Network Interface, CNI), el servidor proxy y los

certificados TLS. Tenga presentes las consideraciones y las concesiones necesarias al implementar la funcionalidad global frente a la funcionalidad por clúster.

Especificación de TkgServiceConfiguration v1alpha2

La especificación `TkgServiceConfiguration` proporciona campos para configurar la instancia de servicio Tanzu Kubernetes Grid.

```
apiVersion: run.tanzu.vmware.com/v1alpha2
kind: TkgServiceConfiguration
metadata:
  name: tkg-service-configuration-spec
spec:
  defaultCNI: string
  proxy:
    httpProxy: string
    httpsProxy: string
    noProxy: [string]
  trust:
    additionalTrustedCAs:
      - name: string
        data: string
  defaultNodeDrainTimeout: time
```

Precaución La configuración de servicio Tanzu Kubernetes Grid es una operación global. Cualquier cambio que realice en la especificación `TkgServiceConfiguration` se aplicará a todos los clústeres de Tanzu Kubernetes aprovisionados por ese servicio. Si se inicia una actualización gradual, ya sea de forma manual o mediante actualización, los clústeres se actualizan según la especificación de servicio modificada.

Especificación de TkgServiceConfiguration v1alpha2 anotada

El siguiente YAML enumera y describe los campos configurables para cada uno de los parámetros de especificación de `TkgServiceConfiguration`. Para ver ejemplos, consulte Ejemplos de configuración de la API de servicio Tanzu Kubernetes Grid v1alpha1.

```
apiVersion: run.tanzu.vmware.com/v1alpha2
kind: TkgServiceConfiguration
metadata:
  name: tkg-service-configuration-spec
spec:
  #defaultCNI is the default CNI for all Tanzu Kubernetes
  #clusters to use unless overridden on a per-cluster basis
  #supported values are antrea, calico, antrea-nsx-routed
  #defaults to antrea
  defaultCNI: string
  #proxy configures a proxy server to be used inside all
  #clusters provisioned by this TKGS instance
  #if implemented all fields are required
  #if omitted no proxy is configured
  proxy:
    #httpProxy is the proxy URI for HTTP connections
```

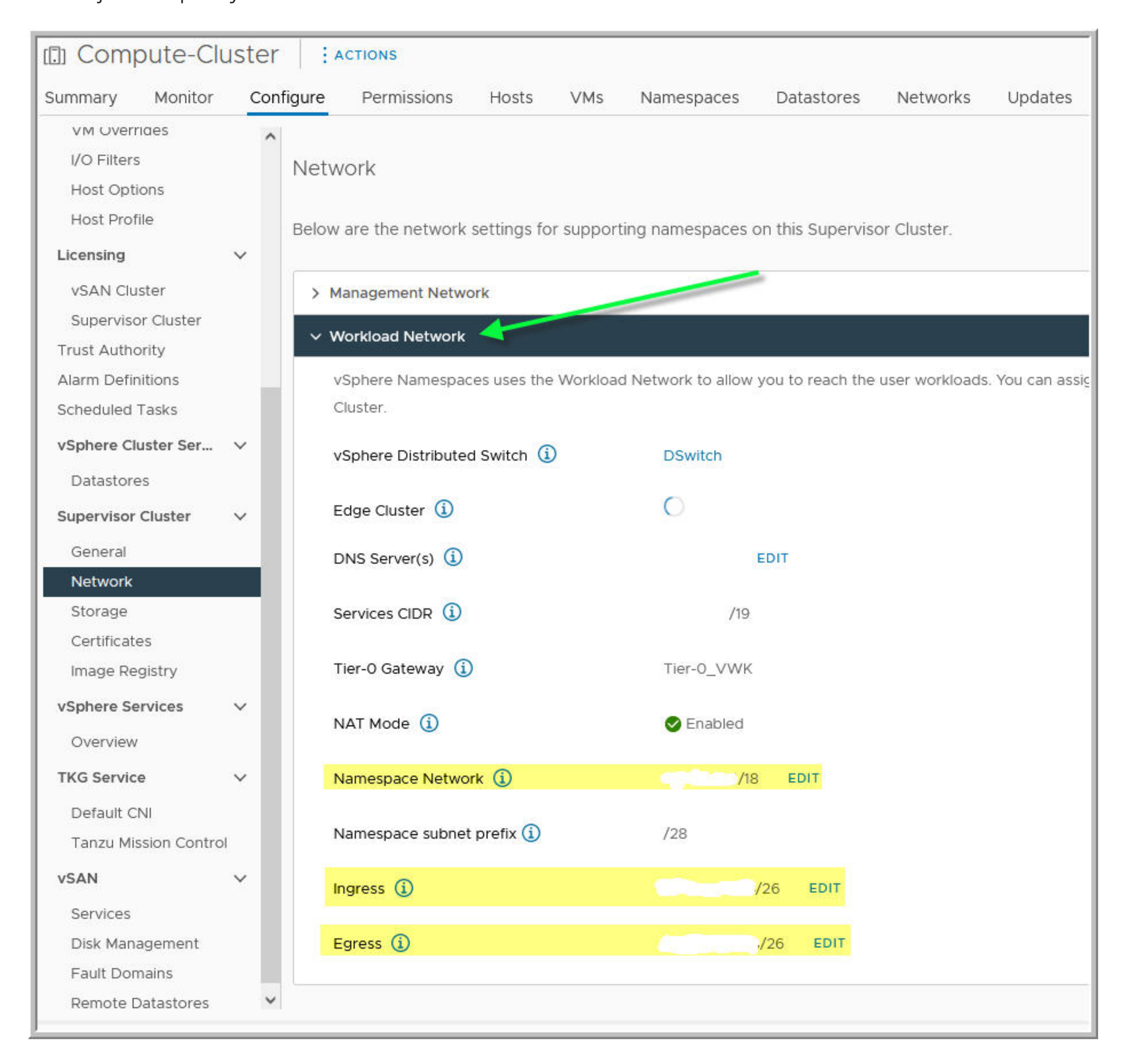
```
    #to endpionts outside the clusters
    #takes the form http://<user>:<pwd>@<ip>:<port>
    httpProxy: string
    #httpsProxy is the proxy URI for HTTPS connections
    #to endpoints outside the clusters
    #takes the frorm http://<user>:<pwd>@<ip>:<port>
    httpsProxy: string
    #noProxy is the list of destination domain names, domains,
    #IP addresses, and other network CIDRs to exclude from proxying
    #must include Supervisor Cluster Pod, Egress, Ingress CIDRs
    noProxy: [string]
  #trust configures additional trusted certificates
  #for the clusters provisioned by this TKGS instance
  #if omitted no additional certificate is configured
  trust:
    #additionalTrustedCAs are additional trusted certificates
    #can be additional CAs or end certificates
    additionalTrustedCAs:
      #name is the name of the additional trusted certificate
      #must match the name used in the filename
      - name: string
        #data holds the contents of the additional trusted cert
        #PEM Public Certificate data encoded as a base64 string
        data: string
  #defaultNodeDrainTimeout is the total amount of time the
  #controller spends draining a node; default is undefined
  #which is the value of 0, meaning the node is drained
  #without any time limitations; note that `nodeDrainTimeout`
  #is different from `kubectl drain --timeout`
  defaultNodeDrainTimeout: time
```

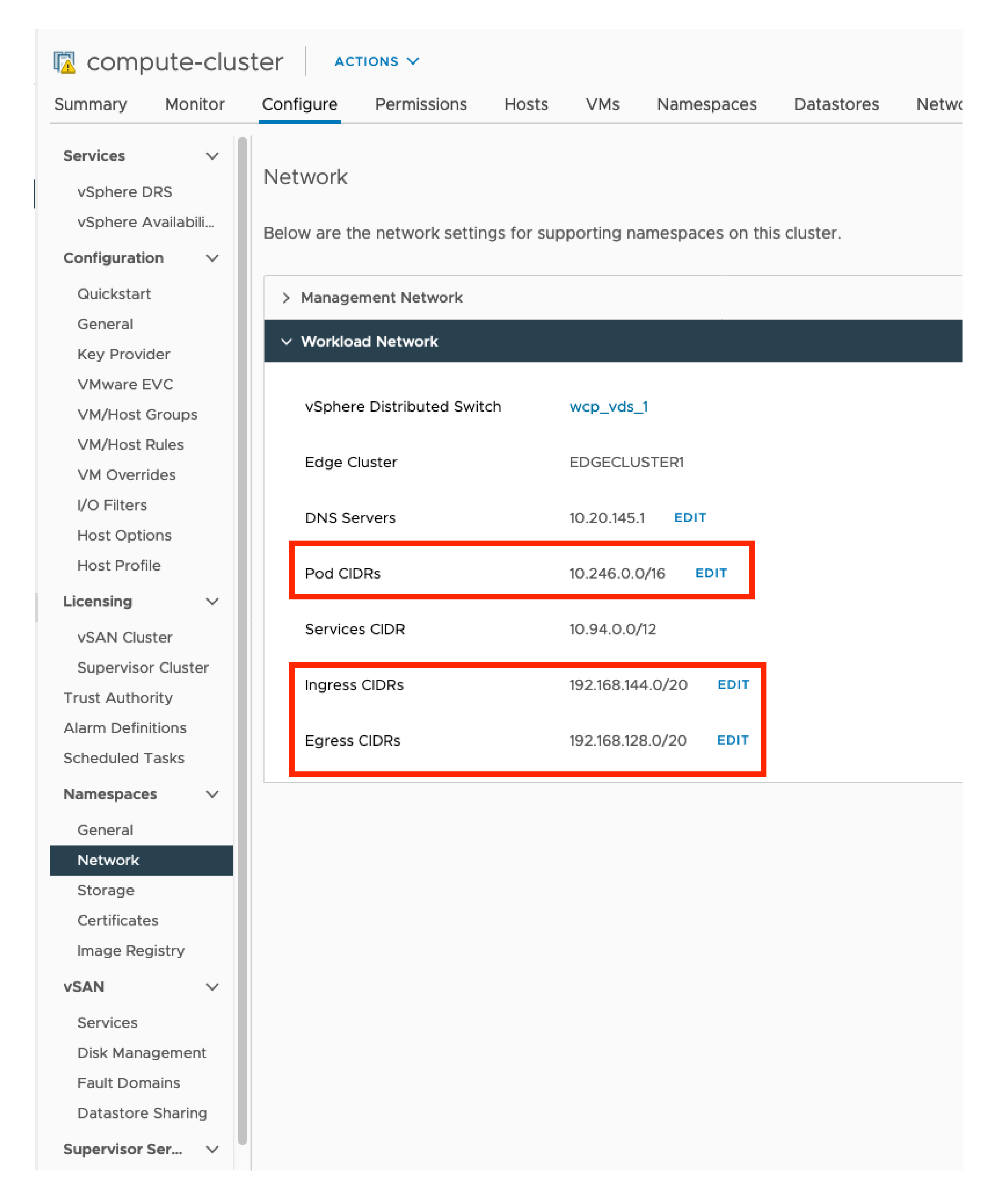
Requisitos de configuración del servidor proxy

Si está configurado, el clúster utilizará el servidor proxy para el tráfico HTTP y HTTPS saliente. Tenga en cuenta los siguientes requisitos para configurar un servidor proxy para los clústeres de Tanzu Kubernetes.

- Los parámetros requeridos del `proxy` son `httpProxy`, `httpsProxy` y `noProxy`. Si agrega la sección `proxy`, los tres campos son obligatorios.
- Puede conectarse al servidor proxy mediante HTTP. No se admiten conexiones HTTPS.
- Los valores de `spec.proxy.noProxy` requeridos se obtienen de la **Red de cargas de trabajo**. No debe usar proxy para la **Red de espacio de nombres** (anteriormente denominada CIDR de pods), la **Entrada** (anteriormente denominada CIDR de entrada) y la **Salida** (anteriormente denominada CIDR de salida) en el campo `noProxy`. Consulte las imágenes de ejemplo a continuación.
- No es necesario incluir los CIDR de servicios en el campo `noProxy`. Los clústeres de Tanzu Kubernetes no interactúan con esta subred.

- No es necesario incluir los valores `network.services.cidrBlocks` y `network.pods.cidrBlocks` de la especificación del clúster de Tanzu Kubernetes en el campo `noProxy`. Estas subredes no son objeto de proxy automáticamente.
- No es necesario incluir `localhost` y `127.0.0.1` en el campo `noProxy`. Los endpoints no son objeto de proxy automáticamente.





Cuándo utilizar las opciones de configuración globales o por clúster

`TkgServiceConfiguration` es una especificación global que afecta a todos los clústeres de Tanzu Kubernetes aprovisionados por la instancia de servicio Tanzu Kubernetes Grid.

Antes de editar `TkgServiceConfiguration`, tenga en cuenta las alternativas por clúster que pueden satisfacer su caso práctico, en lugar de una configuración global.

Tabla 13-2. Opciones de configuración global frente a opciones por clúster

Configuración	Opción global	Opción por clúster
CNI predeterminada	Edite la especificación `TkgServiceConfiguration`. Consulte Ejemplos de configuración de la API de servicio Tanzu Kubernetes Grid v1alpha1.	Especifique la CNI en la especificación del clúster. Por ejemplo, Antrea es la CNI predeterminada. Para usar Calico, especifíquelo en el YAML del clúster. Consulte Ejemplos del aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1.
Servidor proxy	Edite la especificación `TkgServiceConfiguration`. Consulte Ejemplos de configuración de la API de servicio Tanzu Kubernetes Grid v1alpha1.	Incluya los parámetros de configuración del servidor proxy en la especificación del clúster. Consulte Ejemplos del aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1.
Certificados de confianza	Edite la especificación `TkgServiceConfiguration`. Existen dos casos de uso: configurar un registro de contenedor externo y una configuración de proxy basada en certificados. Consulte Ejemplos de configuración de la API de servicio Tanzu Kubernetes Grid v1alpha1.	Sí, puede incluir certificados personalizados por clúster o anular la configuración de `trust` establecida globalmente en la especificación del clúster. Consulte Ejemplos del aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1.

Nota Si se configura un proxy global en `TkgServiceConfiguration`, esa información de proxy se propaga al manifiesto del clúster después de la implementación inicial del clúster. La configuración global del proxy se agrega al manifiesto del clúster solo si no hay ningún campo de configuración de proxy presente cuando se crea el clúster. En otras palabras, la configuración por clúster tiene prioridad y sobrescribirá la configuración global del proxy. Para obtener más información, consulte Parámetros de configuración para la API v1alpha1 de servicio Tanzu Kubernetes Grid.

Antes de editar la especificación `TkgServiceConfiguration`, tenga en cuenta las ramificaciones de aplicar la configuración a nivel global.

Campo	Se aplica	Impacto en los clústeres existentes si se agrega o se cambia	Anulación por clúster al crear un clúster	Anulación por clúster al actualizar un clúster
`defaultCNI`	Globalmente	Ninguno	Sí, puede anular la configuración global al crear el clúster	No, no puede cambiar la CNI de un clúster existente. Si utilizó la CNI predeterminada configurada globalmente al crear el clúster, no puede cambiarla
`proxy`	Globalmente	Ninguno	Sí, puede anular la configuración global al crear el clúster	Sí, con U2+ puede anular la configuración global al actualizar el clúster
`trust`	Globalmente	Ninguno	Sí, puede anular la configuración global al crear el clúster	Sí, con U2+ puede anular la configuración global al actualizar el clúster

Propagar cambios de configuración global a clústeres existentes

La configuración realizada a nivel global en `TkgServiceConfiguration` no se propaga automáticamente a los clústeres existentes. Por ejemplo, si realiza cambios en la configuración de `proxy` o `trust` en `TkgServiceConfiguration`, dichos cambios no afectarán a los clústeres que ya están aprovisionados.

Para propagar un cambio global a un clúster existente, debe aplicar una revisión al clúster de Tanzu Kubernetes para que herede los cambios realizados en `TkgServiceConfiguration`.

Por ejemplo:

```
kubectl patch tkc <CLUSTER_NAME> -n <NAMESPACE> --type merge -p "{\"spec\":{\"settings\":
{\"network\":{\"proxy\": null}}}}"
```

```
kubectl patch tkc <CLUSTER_NAME> -n <NAMESPACE> --type merge -p "{\"spec\":{\"settings\":
{\"network\":{\"trust\": null}}}}"
```

Ejemplos de configuración de la instancia de TKGS mediante la API de v1alpha2

Consulte los ejemplos para personalizar la API de servicio Tanzu Kubernetes Grid v1alpha2 con opciones de configuración global para la interfaz de redes de contenedor (Container Network Interface, CNI), el servidor proxy y los certificados TLS.

Configurar servicio Tanzu Kubernetes Grid mediante la API de v1alpha2

Para personalizar servicio Tanzu Kubernetes Grid, cambie la CNI predeterminada, agregue un servidor proxy global y agregue certificados de confianza. Consulte Parámetros de configuración para la API v1alpha1 de servicio Tanzu Kubernetes Grid.

```
apiVersion: run.tanzu.vmware.com/v1alpha2
kind: TkgServiceConfiguration
metadata:
  name: tkg-service-v2-configuration-example
spec:
  defaultCNI: antrea
  proxy:
    #supported format is `http://<user>:<pwd>@<ip>:<port>`
    httpProxy: http://admin:PaSsWoRd@10.66.100.22:80
    httpsProxy: http://admin:PaSsWoRd@10.66.100.22:80
    noProxy: [10.246.0.0/16,192.168.144.0/20,192.168.128.0/20]
  trust:
    additionalTrustedCAs:
      - name: CompanyInternalCA-1
        data: LS0tLS1C...LS0tCg==
        #where "..." is the middle section of the long base64 string
      - name: CompanyInternalCA-2
        data: MTLtMT1C...MT0tPg==
  defaultNodeDrainTimeout: 0
```

Precaución La edición de la especificación de servicio Tanzu Kubernetes Grid produce cambios globales en todos los clústeres aprovisionados por ese servicio, incluidos los clústeres nuevos y los existentes que se actualizan de forma manual o automática.

Requisito previo: Configurar la edición de Kubectl

Para escalar un clúster de Tanzu Kubernetes, actualice el manifiesto del clúster mediante el comando `kubectl edit tanzukubernetescluster/CLUSTER-NAME`. El comando kubectl edit abre el manifiesto del clúster en el editor de texto definido por las variables de entorno KUBE_EDITOR o EDITOR. Para obtener instrucciones sobre cómo configurar la variable de entorno, consulte Especificar un editor de texto predeterminado para Kubectl.

Al guardar los cambios en la especificación, `kubectl` informa de que las ediciones se registraron correctamente. Para cancelar, simplemente cierre el editor sin guardar.

Configurar la CNI predeterminada

servicio Tanzu Kubernetes Grid proporciona una interfaz de redes de contenedor (Container Network Interface, CNI) predeterminada para los clústeres de Tanzu Kubernetes. La configuración predeterminada permite crear clústeres sin que para ello sea necesario especificar la CNI. Para cambiar el valor de CNI predeterminado, edite la especificación del servicio.

servicio Tanzu Kubernetes Grid admite dos CNI: Antrea y Calico, de las cuales Antrea es la predeterminada. Para obtener más información, consulte Redes de clústeres de servicio Tanzu Kubernetes Grid .

También es posible anular la CNI predeterminada. Para ello, especifique de forma explícita la CNI que se va a utilizar. Como alternativa, puede cambiar la CNI predeterminada mediante la edición del controlador del servicio de TKG para las CNI.

1 Realice la autenticación con clúster supervisor.

```
kubectl vsphere login --server=SVC-IP-ADDRESS --vsphere-username USERNAME
```

2 Cambie el contexto al espacio de nombres de vSphere de destino.

```
kubectl config use-context tkgs-cluster-ns
```

3 Indique la CNI predeterminada.

```
kubectl get tkgserviceconfigurations
```

Resultado de ejemplo:

```

NAME                                  DEFAULT CNI
tkg-service-configuration             antrea
```

4 Cargue para editar la especificación de servicio Tanzu Kubernetes Grid.

```
kubectl edit tkgserviceconfigurations tkg-service-configuration
```

El sistema abre la especificación `tkg-service-configuration` en el editor de texto predeterminado que definen las variables de entorno KUBE_EDITOR o EDITOR.

5 Edite el valor de `spec.defaultCNI`.

Por ejemplo, cambie desde:

```

spec:
  defaultCNI: antrea
```

Cambie a:

```

spec:
  defaultCNI: calico
```

6 Para aplicar los cambios, guarde el archivo en el editor de texto. Para cancelar, cierre el editor sin guardar.

Al guardar el cambio en el editor de texto, kubectl actualiza la especificación de servicio de `tkg-service-configuration`.

7 Compruebe que se haya actualizado la CNI predeterminada.

```
kubectl get tkgserviceconfigurations
```

Se actualiza la CNI predeterminada. Cualquier clúster aprovisionado con la configuración de red predeterminada utiliza la CNI predeterminada.

```
NAME                              DEFAULT CNI
tkg-service-configuration         calico
```

Configurar un servidor proxy global

Para habilitar un servidor proxy global, agregue los parámetros del servidor proxy a `TkgServiceConfiguration`. Si desea ver una descripción de los campos requeridos, consulte Parámetros de configuración para la API v1alpha1 de servicio Tanzu Kubernetes Grid.

1 Realice la autenticación con clúster supervisor.

```
kubectl vsphere login --server=SVC-IP-ADDRESS --vsphere-username USERNAME
```

2 Cambie el contexto al espacio de nombres de vSphere de destino.

```
kubectl config use-context tkgs-cluster-ns
```

3 Obtener la configuración actual.

```
kubectl get tkgserviceconfigurations
```

Resultado de ejemplo:

```
NAME                         DEFAULT CNI
tkg-service-configuration    antrea
```

4 Cargue para editar la especificación de servicio Tanzu Kubernetes Grid.

```
kubectl edit tkgserviceconfigurations tkg-service-configuration
```

El sistema abre la especificación `tkg-service-configuration` en el editor de texto predeterminado que definen las variables de entorno KUBE_EDITOR o EDITOR.

5 Agregue la subsección `spec.proxy` con cada campo que se pide, incluidos `httpProxy`, `httpsProxy` y `noProxy`.

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TkgServiceConfiguration
metadata:
  ...
  name: tkg-service-configuration-example
  resourceVersion: "44170525"
  selfLink: /apis/run.tanzu.vmware.com/v1alpha1/tkgserviceconfigurations/tkg-service-
configuration
  uid: 10347195-5f0f-490e-8ae1-a758a724c0bc
spec:
  defaultCNI: antrea
```

```
  proxy:
    httpProxy: http://<user>:<pwd>@<ip>:<port>
    httpsProxy: http://<user>:<pwd>@<ip>:<port>
    noProxy: [SVC-POD-CIDRs, SVC-EGRESS-CIDRs, SVC-INGRESS-CIDRs]
```

6 Rellene cada campo de proxy con los valores adecuados. Si desea ver una descripción de cada campo, consulte Parámetros de configuración para la API v1alpha1 de servicio Tanzu Kubernetes Grid.

Los valores requeridos para el campo `noProxy` provienen de la **Red de cargas de trabajo** del clúster supervisor. Consulte la imagen en el tema anterior sobre dónde obtener estos valores.

Por ejemplo:

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TkgServiceConfiguration
metadata:
  ...
  name: tkg-service-configuration-example
  resourceVersion: "44170525"
  selfLink: /apis/run.tanzu.vmware.com/v1alpha1/tkgserviceconfigurations/tkg-service-
configuration
  uid: 10347195-5f0f-490e-8ae1-a758a724c0bc
spec:
  defaultCNI: antrea
  proxy:
    httpProxy: http://user:password@10.186.102.224:3128
    httpsProxy: http://user:password@10.186.102.224:3128
    noProxy: [10.246.0.0/16,192.168.144.0/20,192.168.128.0/20]
```

7 Para aplicar los cambios, guarde el archivo en el editor de texto. Para cancelar, cierre el editor sin guardar.

Al guardar los cambios en el editor de texto, kubectl actualiza servicio Tanzu Kubernetes Grid con la configuración definida en la especificación de servicio de `tkg-service-configuration`.

8 Compruebe que el servicio Tanzu Kubernetes Grid se haya actualizado con la configuración del proxy.

```
kubectl get tkgserviceconfigurations -o yaml
```

9 Para comprobarlo, aprovisione el clúster Tanzu Kubernetes. Consulte Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS.

Utilice el siguiente comando para confirmar que el clúster está utilizando el proxy.

```
kubectl get tkc CLUSTER-NAME -n NAMESPACE -o yaml
```

Configuración de un proxy basado en certificados

El uso de un servidor proxy para enrutar el tráfico de Internet es un requisito estricto en algunos entornos. Por ejemplo, una empresa de un sector con muchas regulaciones, como una entidad financiera, requiere que todo el tráfico de Internet pase por un proxy corporativo.

Puede configurar servicio Tanzu Kubernetes Grid para aprovisionar clústeres de Tanzu Kubernetes para que utilicen un servidor proxy para el tráfico HTTP/S saliente. Para obtener más información, consulte Parámetros de configuración para la API v1alpha1 de servicio Tanzu Kubernetes Grid.

Como se muestra en el ejemplo, puede agregar certificados de confianza para el servidor proxy a la especificación `TkgServiceConfiguration`.

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TkgServiceConfiguration
metadata:
  name: tkg-service-configuration-example
spec:
  defaultCNI: antrea
  proxy:
    httpProxy: http://user:password@10.186.102.224:3128
    httpsProxy: http://user:password@10.186.102.224:3128
    noProxy: [10.246.0.0/16,192.168.144.0/20,192.168.128.0/20]
  trust:
    additionalTrustedCAs:
      - name: first-cert-name
        data: base64-encoded string of a PEM encoded public cert 1
      - name: second-cert-name
        data: base64-encoded string of a PEM encoded public cert 2
  defaultNodeDrainTimeout: 0
```

Configuración del registro privado externo

Puede configurar servicio Tanzu Kubernetes Grid con certificados personalizados para conectar clústeres de Tanzu Kubernetes con un registro privado externo. Para obtener más información, consulte Usar un registro de contenedor externo con clústeres de Tanzu Kubernetes.

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TkgServiceConfiguration
metadata:
  name: tkg-service-configuration-example
spec:
  defaultCNI: antrea
  trust:
    additionalTrustedCAs:
      - name: harbor-vm-cert
        data: <<<base64-encoded string of a PEM encoded public cert>>>>
```

Ampliar un clúster de Tanzu Kubernetes mediante la API v1alpha2 de TKGS

Puede ampliar un clúster de Tanzu Kubernetes horizontalmente cambiando el número de nodos o verticalmente, cambiando la clase de máquina virtual que aloja los nodos.

Operaciones de ampliación admitidas

En la tabla se enumeran las operaciones de ampliación admitidas para clústeres de Tanzu Kubernetes.

Tabla 13-3. Operaciones de ampliación admitidas para clústeres de Tanzu Kubernetes

Nodo	Expansión horizontal	Reducción horizontal	Ampliación vertical	Escala de volumen
Plano de control	Sí	No	Sí	No
Trabajador	Sí	Sí	Sí	Sí

Tenga en cuenta las siguientes consideraciones:

- Al ampliar verticalmente un nodo de clúster, es posible que las cargas de trabajo ya no puedan ejecutarse en el nodo por falta de recursos disponibles. Por esta razón, puede que la ampliación horizontal sea el método preferido.
- Las clases de máquina virtual no son inmutables. Si se escala horizontalmente un clúster de Tanzu Kubernetes después de editar una clase de máquina virtual utilizada por ese clúster, los nuevos nodos del clúster utilizan la definición de clase actualizada, pero los nodos del clúster existentes siguen usando la definición de clase inicial, lo que provoca un error de coincidencia. Consulte Clases de máquina virtual para clústeres de Tanzu Kubernetes.
- Los volúmenes del nodo de trabajo se pueden cambiar después del aprovisionamiento, pero no los volúmenes de los nodos del plano de control.

Requisito previo para la ampliación: configurar la edición de Kubectl

Para escalar un clúster de Tanzu Kubernetes, actualice el manifiesto del clúster mediante el comando `kubectl edit tanzukubernetescluster/CLUSTER-NAME`. El comando kubectl edit abre el manifiesto del clúster en el editor de texto definido por las variables de entorno KUBE_EDITOR o EDITOR. Para obtener instrucciones sobre cómo configurar la variable de entorno, consulte Especificar un editor de texto predeterminado para Kubectl.

Al guardar los cambios del manifiesto, `kubectl` informa que las modificaciones se registraron correctamente, y el clúster se actualiza con los cambios.

```
kubectl edit tanzukubernetescluster/tkgs-cluster-1
tanzukubernetescluster.run.tanzu.vmware.com/tkgs-cluster-1 edited
```

Para cancelar, simplemente cierre el editor sin guardar.

```
kubectl edit tanzukubernetescluster/tkgs-cluster-1
Edit cancelled, no changes made.
```

Ampliar horizontalmente el plano de control

Para ampliar horizontalmente un clúster de Tanzu Kubernetes, aumente el número de nodos del plano de control de 1 a 3. El número de nodos del plano de control debe ser impar. No se puede realizar una ampliación vertical en el plano de control.

1 Realice la autenticación con clúster supervisor.

```
kubectl vsphere login --server=SVC-IP-ADDRESS --vsphere-username USERNAME
```

2 Cambie el contexto al espacio de nombres de vSphere en el que se aprovisiona el clúster de Tanzu Kubernetes.

```
kubectl config use-context tkgs-cluster-ns
```

3 Enumere los clústeres de Kubernetes que se están ejecutando en el espacio de nombres.

```
kubectl get tanzukubernetescluster -n tkgs-cluster-ns
```

4 Obtenga la cantidad de nodos que se ejecutan en el clúster de destino.

```
kubectl get tanzukubernetescluster tkgs-cluster-1
```

Por ejemplo, el siguiente clúster tiene 1 nodo de plano de control y 3 nodos de trabajo.

```

NAMESPACE             NAME             CONTROL PLANE   WORKER   TKR
NAME                           AGE     READY
tkgs-cluster-ns       test-cluster     1               3        v1.21.2---vmware.1-
tkg.1.13da849   5d12h   True
```

5 Cargue el manifiesto del clúster para editarlo ejecutando el comando `kubectl edit`.

```
kubectl edit tanzukubernetescluster/tkgs-cluster-1
```

El manifiesto del clúster se abrirá en el editor de texto que definan las variables de entorno KUBE_EDITOR o EDITOR.

6 Busque el parámetro `spec.topology.controlPlane.count` y aumente el número de nodos de 1 a 3.

```
...
controlPlane:
    replicas: 1
...
```

```
...
ControlPlane:
    replicas: 3
...
```

7 Para aplicar los cambios, guarde el archivo en el editor de texto. Para cancelar, cierre el editor sin guardar.

Cuando guarde el archivo, kubectl aplicará los cambios al clúster. En segundo plano, el servicio de máquina virtual del clúster supervisor aprovisiona el nuevo nodo de trabajo.

8 Compruebe que se agreguen los nodos nuevos.

```
kubectl get tanzukubernetescluster tkgs-cluster-1
```

El plano de control que se amplió horizontalmente ahora tiene 3 nodos.

```
NAMESPACE             NAME             CONTROL PLANE   WORKER   TKR
NAME                           AGE     READY
tkgs-cluster-ns       test-cluster     3               3        v1.21.2---vmware.1-
tkg.1.13da849   5d12h   True
```

Escalar horizontalmente los nodos de trabajo

Para escalar horizontalmente un clúster de Tanzu Kubernetes, aumente el número de nodos de trabajo mediante kubectl.

1 Realice la autenticación con clúster supervisor.

```
kubectl vsphere login --server=SVC-IP-ADDRESS --vsphere-username USERNAME
```

2 Cambie el contexto al espacio de nombres de vSphere en el que se aprovisiona el clúster de Tanzu Kubernetes.

```
kubectl config use-context tkgs-cluster-ns
```

3 Enumere los clústeres de Kubernetes que se están ejecutando en el espacio de nombres.

```
kubectl get tanzukubernetescluster -n tkgs-cluster-ns
```

4 Obtenga la cantidad de nodos que se ejecutan en el clúster de destino.

```
kubectl get tanzukubernetescluster tkgs-cluster-1
```

Por ejemplo, el siguiente clúster tiene 3 nodo de plano de control y 3 nodos de trabajo.

```
NAMESPACE             NAME             CONTROL PLANE   WORKER   TKR
NAME                           AGE     READY
tkgs-cluster-ns       test-cluster     3               3        v1.21.2---vmware.1-
tkg.1.13da849   5d12h   True
```

5 Cargue el manifiesto del clúster para editarlo ejecutando el comando `kubectl edit`.

```
kubectl edit tanzukubernetescluster/tkgs-cluster-1
```

El manifiesto del clúster se abrirá en el editor de texto que definan las variables de entorno KUBE_EDITOR o EDITOR.

6 Busque el parámetro `spec.topology.workers.count` y aumente el número de nodos.

```
...
workers:
    replicas: 3
...
```

```
...
workers:
    replicas: 4
...
```

7 Para aplicar los cambios, guarde el archivo en el editor de texto. Para cancelar, cierre el editor sin guardar.

Cuando guarde el archivo, kubectl aplicará los cambios al clúster. En segundo plano, el servicio de máquina virtual del clúster supervisor aprovisiona el nuevo nodo de trabajo.

8 Compruebe que se haya agregado el nuevo nodo de trabajo.

```
kubectl get tanzukubernetescluster tkgs-cluster-1
```

Después de ampliar, el clúster tiene 4 nodos de trabajo.

```

NAMESPACE             NAME             CONTROL PLANE   WORKER   TKR
NAME                          AGE      READY
tkgs-cluster-ns       test-cluster     3               4        v1.21.2---vmware.1-
tkg.1.13da849   5d12h   True
```

Reducir los nodos de trabajo

Para reducir un clúster de Tanzu Kubernetes, reduzca el número de nodos de trabajo. No se admite la reducción en el plano de control.

1 Realice la autenticación con clúster supervisor.

```
kubectl vsphere login --server=SVC-IP-ADDRESS --vsphere-username USERNAME
```

2 Cambie el contexto al espacio de nombres de vSphere en el que se aprovisiona el clúster de Tanzu Kubernetes.

```
kubectl config use-context tkgs-cluster-ns
```

3 Enumere los clústeres de Kubernetes que se están ejecutando en el espacio de nombres.

```
kubectl get tanzukubernetescluster -n tkgs-cluster-ns
```

4 Obtenga la cantidad de nodos que se ejecutan en el clúster de destino.

```
kubectl get tanzukubernetescluster tkgs-cluster-1
```

Por ejemplo, el siguiente clúster tiene 3 nodo de plano de control y 4 nodos de trabajo.

```
NAMESPACE             NAME            CONTROL PLANE   WORKER   TKR
NAME                           AGE     READY
tkgs-cluster-ns       test-cluster    3               4        v1.21.2---vmware.1-
tkg.1.13da849   5d12h   True
```

5 Cargue el manifiesto del clúster para editarlo ejecutando el comando `kubectl edit`.

```
kubectl edit tanzukubernetescluster/tkgs-cluster-1
```

El manifiesto del clúster se abrirá en el editor de texto que definan las variables de entorno KUBE_EDITOR o EDITOR.

6 Busque el parámetro `spec.topology.workers.count` y reduzca el número de nodos.

```
...
workers:
    replicas: 4
...
```

```
...
workers:
    replicas: 2
...
```

7 Para aplicar los cambios, guarde el archivo en el editor de texto. Para cancelar, cierre el editor sin guardar.

Cuando guarde el archivo, kubectl aplicará los cambios al clúster. En segundo plano, el servicio de máquina virtual del clúster supervisor aprovisiona el nuevo nodo de trabajo.

8 Compruebe que se hayan agregado los nodos de trabajo.

```
kubectl get tanzukubernetescluster tkgs-cluster-1
```

Después de reducir, el clúster tiene 2 nodos de trabajo.

```
NAMESPACE             NAME            CONTROL PLANE   WORKER   TKR
NAME                           AGE     READY
tkgs-cluster-ns       test-cluster    3               2        v1.21.2---vmware.1-
tkg.1.13da849   5d12h   True
```

Ampliar un clúster verticalmente

Puede ampliar verticalmente un clúster de Tanzu Kubernetes si cambia la clase de máquina virtual que se utiliza para alojar los nodos del clúster. El ajuste de ampliación vertical es compatible con los nodos de plano de control y de trabajo.

servicio Tanzu Kubernetes Grid admite el escalado vertical de nodos del clúster a través del mecanismo de actualización gradual que está integrado en el servicio. Si cambia la definición de `VirtualMachineClass`, el servicio implementa gradualmente los nodos nuevos con esa nueva clase y reduce la velocidad de los nodos antiguos. Consulte Actualizar clústeres de Tanzu Kubernetes.

1 Realice la autenticación con clúster supervisor.

```
kubectl vsphere login --server=SVC-IP-ADDRESS --vsphere-username USERNAME
```

2 Cambie el contexto al espacio de nombres de vSphere en el que se aprovisiona el clúster de Tanzu Kubernetes.

```
kubectl config use-context tkgs-cluster-ns
```

3 Enumere los clústeres de Kubernetes que se están ejecutando en el espacio de nombres.

```
kubectl get tanzukubernetescluster -n tkgs-cluster-ns
```

4 Describa el clúster de Tanzu Kubernetes de destino y compruebe la clase de máquina virtual.

```
kubectl describe tanzukubernetescluster tkgs-cluster-2
```

Por ejemplo, el siguiente clúster utiliza la clase de máquina virtual best-effort-medium.

```
Spec:
  ...
  Topology:
    Control Plane:
      Class:          best-effort-medium
      ...
    nodePool-a1:
      Class:          best-effort-medium
      ...
```

5 Enumere y describa las clases de máquinas virtuales disponibles.

```
kubectl get virtualmachineclassbinding
```

```
kubectl describe virtualmachineclassbinding
```

Nota La clase de máquina virtual que desea utilizar debe estar enlazada al espacio de nombres de vSphere. Consulte Clases de máquina virtual para clústeres de Tanzu Kubernetes.

6 Abra para editar el manifiesto del clúster de destino.

```
kubectl edit tanzukubernetescluster/tkgs-cluster-2
```

El manifiesto del clúster se abrirá en el editor de texto que definan las variables de entorno KUBE_EDITOR o EDITOR.

7 Edite el manifiesto cambiando la clase de máquina virtual.

Por ejemplo, edite el manifiesto del clúster para usar la clase de máquina virtual `guaranteed-large` para el plano de control y los nodos de trabajo.

```
spec:
  topology:
    controlPlane:
      class: guaranteed-large
      ...
    nodePool-a1:
      class: guaranteed-large
      ...
```

8 Para aplicar los cambios, guarde el archivo en el editor de texto. Para cancelar, cierre el editor sin guardar.

Cuando guarde el archivo, kubectl aplicará los cambios al clúster. En segundo plano, servicio Tanzu Kubernetes Grid aprovisiona los nuevos nodos y elimina los anteriores. Si desea ver una descripción del proceso de actualización gradual, consulte Acerca de las actualizaciones de clústeres de servicio Tanzu Kubernetes Grid.

9 Compruebe que el clúster se haya actualizado.

```
kubectl get tanzukubernetescluster
NAMESPACE             NAME            CONTROL PLANE   WORKER   TKR
NAME                           AGE     READY
tkgs-cluster-ns       test-cluster    3               3        v1.21.2---vmware.1-
tkg.1.13da849   5d12h   True
```

Escalar volúmenes de nodos

En la especificación de clúster de Tanzu Kubernetes para los nodos, tiene la opción de declarar uno o varios volúmenes persistentes. La declaración de un volumen de nodo es útil para los componentes de alta rotación, como la base de datos ectd en el plano de control y el tiempo de ejecución del contenedor en los nodos de trabajo. A continuación se proporciona un extracto de la especificación del clúster con ambos volúmenes de nodo declarados como referencia. (Un ejemplo completo de especificación de clúster está disponible YAML de ejemplo para el aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS).

Si desea agregar o cambiar uno o más volúmenes de nodos después de la creación del clúster, tenga en cuenta las siguientes consideraciones:

Nodo de volumen	Descripción
Se permiten cambios en el volumen del nodo de trabajo.	Después de aprovisionar un clúster de Tanzu Kubernetes, puede agregar o actualizar un volumen de nodo de trabajo. Cuando se inicia una actualización gradual, el clúster se actualiza con el volumen nuevo o cambiado. **Advertencia** Si escala el nodo de trabajo con un volumen nuevo o modificado, los datos del volumen actual se eliminan durante la actualización gradual.
No se permiten cambios en el volumen del nodo del plano de control.	Después de aprovisionar un clúster de Tanzu Kubernetes, no se puede agregar ni actualizar un volumen de nodo de plano de control. La API de clúster de Kubernetes (CAPI) prohíbe los cambios posteriores a la creación en `spec.toplogy.controlPlane.volumes`. Si intenta agregar o cambiar un volumen del plano de control después de la creación del clúster, se rechaza la solicitud y se recibe el mensaje de error "No se permiten las actualizaciones de los campos inmutables".

```
spec:
  topology:
    controlPlane:
      replicas: 3
      vmClass: guaranteed-medium
      storageClass: vwt-storage-policy
      volumes:
        - name: etcd
          mountPath: /var/lib/etcd
          capacity:
            storage: 4Gi
      tkr:
        reference:
          name: v1.21.2---vmware.1-tkg.1.ee25d55
    nodePools:
    - name: worker-nodepool-a1
      replicas: 3
      vmClass: guaranteed-large
      storageClass: vwt-storage-policy
      volumes:
        - name: containerd
          mountPath: /var/lib/containerd
          capacity:
            storage: 16Gi
```

Aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha1 de servicio Tanzu Kubernetes Grid

En esta sección se describe cómo aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha1 de servicio Tanzu Kubernetes Grid.

Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha1 de servicio Tanzu Kubernetes Grid

Para aprovisionar clústeres de Tanzu Kubernetes, se debe invocar a la API declarativa de servicio Tanzu Kubernetes Grid mediante kubectl y una especificación de clúster definida mediante YAML. Después de aprovisionar un clúster, puede usarlo e implementar cargas de trabajo en él mediante kubectl.

El flujo de trabajo proporciona un procedimiento de extremo a extremo para el proceso de aprovisionamiento del clúster. Cada uno de los pasos tiene vínculos con los que se puede obtener más información sobre la tarea específica.

Requisitos previos

Complete los siguientes requisitos previos:

- Configure una instancia de clúster supervisor. Consulte Capítulo 5 Configurar y administrar un clúster supervisor.
- Cree un espacio de nombres de vSphere en el que planee aprovisionar clústeres de Tanzu Kubernetes. Consulte Creación y configuración de un espacio de nombres de vSphere.

  La configuración inicial del espacio de nombres requiere lo siguiente:

  - Permisos de edición a uno o varios ingenieros de Desarrollo y operaciones para que accedan al espacio de nombres con credenciales de vCenter Single Sign-On.
  - Directiva de almacenamiento compartido basada en etiquetas para el espacio de nombres.
  - Las cuotas de capacidad y uso para el espacio de nombres se verifican y ajustan según sea necesario.
- Cree una biblioteca de contenido para versiones de Tanzu Kubernetes en un almacén de datos compartido y sincronice las versiones que desea utilizar. Consulte Crear y administrar bibliotecas de contenido para versiones de Tanzu Kubernetes.
- Asocie la biblioteca de contenido y las clases de máquinas virtuales con el espacio de nombres de vSphere. Consulte Configurar un espacio de nombres de vSphere para las versiones de Tanzu Kubernetes.

Procedimiento

1. Descargue e instale las Herramientas de la CLI de Kubernetes para vSphere. Consulte Descargar e instalar Herramientas de la CLI de Kubernetes para vSphere.
2. Utilice complemento de vSphere para kubectl para autenticarse en clúster supervisor. Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

   ```
   kubectl vsphere login --server=IP-ADDRESS --vsphere-username USERNAME
   ```

3 Con kubectl, cambie el contexto a la instancia de espacio de nombres de vSphere donde tiene previsto aprovisionar el clúster de Tanzu Kubernetes.

```
kubectl config get-contexts
```

```
kubectl config use-context SUPERVISOR-NAMESPACE
```

Por ejemplo:

```
kubectl config use-context tkgs-cluster-ns
```

4 Enumere los enlaces de clase de máquina virtual disponibles. Consulte Clases de máquina virtual para clústeres de Tanzu Kubernetes.

Utilice el siguiente comando para enumerar todos los enlaces de clase de máquina virtual que están disponibles en espacio de nombres de vSphere donde se implementa el clúster.

```
kubectl get virtualmachineclassbindings
```

Nota El comando `kubectl get virtualmachineclasses` enumera todas las clases de máquina virtual presentes en el clúster supervisor. Debido a que debe asociar las clases de máquina virtual con el espacio de nombres de vSphere, solo puede usar las clases de máquina virtual que están enlazadas al espacio de nombres de destino.

5 Obtenga la clase de almacenamiento predeterminada disponible mediante la descripción del espacio de nombres.

```
kubectl describe namespace SUPERVISOR-NAMESPACE
```

6 Lista de versiones de Tanzu Kubernetes disponibles:

Nota Consulte la lista de versiones de versiones de Tanzu Kubernetes para obtener información sobre la compatibilidad. Consulte Comprobar la compatibilidad del clúster de Tanzu Kubernetes para actualizar.

```
kubectl get tanzukubernetesreleases
```

Nota El comando `kubectl get virtualmachineimages` devuelve información genérica sobre las máquinas virtuales.

7 Cree el archivo YAML para el aprovisionamiento de un clúster de Tanzu Kubernetes.

   a Comience con uno de los archivos YAML de ejemplo. Consulte Ejemplos del aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1.

      Por ejemplo, el siguiente archivo YAML aprovisiona un clúster mínimo con todos los valores predeterminados del clúster disponibles:

```
apiVersion: run.tanzu.vmware.com/v1alpha1  #TKGS API endpoint
kind: TanzuKubernetesCluster               #required parameter
metadata:
  name: tkgs-cluster-1                     #cluster name, user defined
  namespace: tgks-cluster-ns               #vsphere namespace
spec:
  distribution:
    version: v1.19                         #Resolves to latest TKR 1.19 version
  topology:
    controlPlane:
      count: 1                             #number of control plane nodes
      class: best-effort-medium            #vmclass for control plane nodes
      storageClass: vwt-storage-policy     #storageclass for control plane
    workers:
      count: 3                             #number of worker nodes
      class: best-effort-medium            #vmclass for worker nodes
      storageClass: vwt-storage-policy     #storageclass for worker nodes
```

   b Utilice la información que resaltó de los resultados de los comandos anteriores para rellenar el YAML del clúster, incluido el espacio de nombres, la clase de almacenamiento y la clase de máquina virtual.

   c Personalice el clúster según sea necesario haciendo referencia a la lista completa de parámetros de configuración del clúster. Consulte Parámetros de configuración para clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1.

   d Guarde el archivo como `tkgs-cluster-1.yaml` o un formato similar.

8 Ejecute el siguiente comando kubectl para aprovisionar el clúster.

```
kubectl apply -f CLUSTER-NAME.yaml
```

   Por ejemplo:

```
kubectl apply -f tkgs-cluster-1.yaml
```

   Resultado esperado:

```
tanzukubernetescluster.run.tanzu.vmware.com/tkgs-cluster-1 created
```

9 Supervise la implementación de nodos del clúster mediante kubectl. Consulte Supervisar el estado del clúster de Tanzu Kubernetes mediante kubectl.

```
kubectl get tanzukubernetesclusters
```

Resultado de ejemplo:

```
NAME             CONTROL PLANE   WORKER   DISTRIBUTION                       AGE     PHASE
tkgs-cluster-2   1               3        v1.19.7+vmware.1-tkg.1.c40d30d    7m59s   running
```

10 Supervise la implementación de nodos del clúster mediante vSphere Client. Consulte Supervisar el estado del clúster de Tanzu Kubernetes mediante vSphere Client.

Por ejemplo, en el inventario de vSphere, debería ver los nodos de máquina virtual que se implementan en el espacio de nombres.

11 Ejecute comandos adicionales para verificar el aprovisionamiento de clústeres. Consulte Usar comandos operativos del clúster de Tanzu Kubernetes.

Por ejemplo:

```
kubectl get tanzukubernetescluster,cluster-
api,virtualmachinesetresourcepolicy,virtualmachineservice,virtualmachine
```

Nota Para obtener más soluciones de problemas, consulte Solución de problemas de clústeres de Tanzu Kubernetes.

12 Con complemento de vSphere para kubectl, inicie sesión en el clúster. Consulte Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.

```
kubectl vsphere login --server=IP-ADDRESS --vsphere-username USERNAME \
--tanzu-kubernetes-cluster-name CLUSTER-NAME --tanzu-kubernetes-cluster-namespace
NAMESPACE-NAME
```

13 Compruebe el aprovisionamiento de clústeres mediante los siguientes comandos de kubectl.

```
kubectl cluster-info
```

```
kubectl get nodes
```

```
kubectl get namespaces
```

```
kubectl api-resources
```

14 Implemente un ejemplo de carga de trabajo y compruebe la creación de clústeres. Consulte Implementar cargas de trabajo en clústeres de Tanzu Kubernetes.

Nota Los clústeres de Tanzu Kubernetes tienen habilitada la directiva de seguridad de pods. Según la carga de trabajo y el usuario, es posible que deba crear un objeto RoleBinding adecuado o un objeto PodSecurityPolicy personalizado. Consulte Usar las directivas de seguridad de pods con clústeres de Tanzu Kubernetes.

15 Implemente extensiones de TKG para hacer que el clúster se implemente de forma operativa. Consulte Implementar paquetes TKG en clústeres de Tanzu Kubernetes.

Parámetros de configuración para clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1

La API declarativa de servicio Tanzu Kubernetes Grid expone varios parámetros para configurar clústeres de Tanzu Kubernetes. Consulte la lista y la descripción de todos los parámetros, y las directrices de uso para aprovisionar y personalizar los clústeres.

YAML con anotaciones para aprovisionar un clúster de Tanzu Kubernetes

El YAML con anotaciones enumera todos los parámetros disponibles para aprovisionar un clúster de Tanzu Kubernetes y tiene comentarios resumidos para cada campo.

Nota El YAML con anotaciones no se valida para aprovisionar un clúster. Consulte los ejemplos para obtener instrucciones sobre ese tema: Ejemplos del aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1.

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TanzuKubernetesCluster
metadata:
  name: <tanzu kubernetes cluster name>
  namespace: <vsphere namespace where the cluster will be provisioned>
spec:
  distribution:
    version: <tanzu kubernetes release version string: full, point, short>
  topology:
    controlPlane:
      count: <integer either 1 or 3>
      class: <vm class bound to the target vsphere namespace>
      storageClass: <vsphere storage policy bound to the target vsphere namespace>
      volumes: #optional setting for high-churn control plane component (such as etcd)
        - name: <user-defined string>
          mountPath: </dir/path>
          capacity:
            storage: <size in GiB>
    workers:
      count: <integer from 0 to 150>
      class: <vm class bound to the target vsphere namespace>
      storageClass: <vsphere storage policy bound to the target vsphere namespace>
      volumes: #optional setting for high-churn worker node component (such as containerd)
```

```
        - name: <user-defined string>
          mountPath: </dir/path>
          capacity:
            storage: <size in GiB>
  settings: #all spec.settings are optional
    storage: #optional storage settings
      classes: [<array of kubernetes storage classes for dynamic pvc provisioning>]
      defaultClass: <default kubernetes storage class>
    network: #optional network settings
      cni: #override default cni set in the tkgservicesonfiguration spec
        name: <antrea or calico>
      pods: #custom pod network
        cidrBlocks: [<array of pod cidr blocks>]
      services: #custom service network
        cidrBlocks: [<array of service cidr blocks>]
      serviceDomain: <custom service domain>
      proxy: #proxy server for outbound connections
        httpProxy: http://<IP:PORT>
        httpsProxy: http://<IP:PORT>
        noProxy: [<array of CIDRs to not proxy>]
      trust: #trust fields for custom public certs for tls
        additionalTrustedCAs:
          - name: <first-cert-name>
            data: <base64-encoded string of PEM encoded public cert 1>
          - name: <second-cert-name>
            data: <base64-encoded string of PEM encoded public cert 2>
```

Parámetros para aprovisionar clústeres de Tanzu Kubernetes

En la tabla se enumeran y describen todos los parámetros y los valores aceptables para aprovisionar un clúster de Tanzu Kubernetes. Para ver ejemplos, consulte Ejemplos de configuración de la API de servicio Tanzu Kubernetes Grid v1alpha1.

Tabla 13-4. Parámetros para aprovisionar clústeres de Tanzu Kubernetes

Nombre	Valor	Descripción
apiVersion	run.tanzu.vmware.com/v1alpha1	Especifica la versión de la API del servicio Tanzu Kubernetes Grid.
kind	TanzuKubernetesCluster	Especifica el tipo de recurso de Kubernetes que se debe crear. El único valor permitido es TanzuKubernetesCluster (distingue entre mayúsculas y minúsculas).
metadata	Sección para los metadatos del clúster	Incluye metadatos del clúster, como name y namespace. Estos son metadatos estándar de Kubernetes, por lo que puede utilizar generateName en lugar de name, agregar etiquetas y anotaciones, etc.

Tabla 13-4. Parámetros para aprovisionar clústeres de Tanzu Kubernetes (continuación)

Nombre	Valor	Descripción
`name`	Una cadena definida por el usuario que acepta caracteres alfanuméricos y guiones (por ejemplo, `my-tkg-cluster-1`)	Especifica el nombre del clúster que se creará. Restricciones de nomenclatura actuales del clúster: ■ El nombre debe tener 41 caracteres o menos. ■ El nombre debe comenzar con una letra. ■ El nombre puede contener letras, números y guiones. ■ El nombre debe terminar con una letra o un número.
`namespace`	Una cadena definida por el usuario que acepta caracteres alfanuméricos y guiones (por ejemplo, `my-sns-1`)	Identifica el nombre del espacio de nombres de supervisor en el que se implementará el clúster. Esta es una referencia a un espacio de nombres de supervisor que existe en el clúster supervisor.
`spec`	Sección para las especificaciones técnicas del clúster	Incluye la especificación (expresada de manera declarativa) para el estado final del clúster, incluidas las instancias de `toplogy` del nodo y de `distribution` del software de Kubernetes.
`distribution`	Sección para especificar la versión de Tanzu Kubernetes Release	Indica la distribución del clúster: el software de clústeres de Tanzu Kubernetes instalado en el plano de control y los nodos de trabajo, incluido Kubernetes.
`version`	Una cadena alfanumérica con guiones que representa la versión de Kubernetes (por ejemplo, `v1.20.2+vmware.1-tkg.1`, `v1.20.2` o `v1.20`)	Especifica la versión de software de la distribución de Kubernetes que se instalará en los nodos del clúster mediante una notación de versión semántica. Puede especificar la versión completa o utilizar abreviaturas de versiones, como "version: v1.20.2", que se resuelve como la imagen más reciente que coincide con esa versión de revisión, o como "version: v1.20", que se resuelve como la versión de revisión que coincide más reciente. La versión resuelta se muestra como "fullVersion" en la descripción del clúster después de crearla.

Tabla 13-4. Parámetros para aprovisionar clústeres de Tanzu Kubernetes (continuación)

Nombre	Valor	Descripción
`topology`	Sección para topologías de nodo del clúster	Incluye campos en los que se describen la cantidad, el propósito y la organización de nodos del clúster, así como los recursos asignados a cada uno. Los nodos del clúster se colocan en grupos en función de su propósito previsto: `control-plane` o `worker`. Cada grupo es homogéneo, tiene la misma asignación de recursos y utiliza el mismo almacenamiento.
`controlPlane`	Sección para la configuración del plano de control	Especifica la topología del plano de control del clúster, incluidos el número de nodos (`count`), el tipo de máquina virtual (`class`) y los recursos de almacenamiento asignados a cada nodo (`storageClass`).
`count`	Un entero igual a `1` o `3`	Especifica el número de nodos del plano de control. El plano de control debe tener un número impar de nodos.
`class`	Un elemento definido por el sistema en forma de cadena de un conjunto enumerado (por ejemplo, `guaranteed-small` o `best-effort-large`)	Especifica el nombre del elemento VirtualMachineClass que describe la configuración de hardware virtual que se utilizará en cada nodo del grupo. Esto controla el hardware disponible para el nodo (CPU y memoria), así como las solicitudes y los límites de dichos recursos. Consulte Clases de máquina virtual para clústeres de Tanzu Kubernetes.

Tabla 13-4. Parámetros para aprovisionar clústeres de Tanzu Kubernetes (continuación)

Nombre	Valor	Descripción
`storageClass`	`node-storage` (por ejemplo)	Identifica la clase de almacenamiento que se utilizará para almacenar los discos que contienen los sistemas de archivos raíz de los nodos de plano de control. Ejecute `kubectl describe ns` en el espacio de nombres para ver las clases de almacenamiento disponibles. Las clases de almacenamiento disponibles para el espacio de nombres varían según el almacenamiento que establece el administrador de vSphere. Las clases de almacenamiento asociadas con el espacio de nombres de supervisor se replican en el clúster. En otras palabras, la clase de almacenamiento debe estar disponible en el espacio de nombres de supervisor para que sea un valor válido para este campo. Consulte Capítulo 7 Configurar y administrar los espacios de nombres de vSphere.
`volumes`	Configuración de almacenamiento opcional ■ volúmenes: ■ nombre: *string* ■ mountPath: */dir/path* ■ capacidad ■ almacenamiento: tamaño de GiB	Puede especificar parámetros de almacenamiento y disco independientes para etcd en los nodos del plano de control. Consulte el ejemplo Clúster con discos y parámetros de almacenamiento independientes.
`workers`	Sección para la configuración de nodos de trabajo	Especifica la topología de los nodos de trabajo del clúster, incluidos el número de nodos (`count`), el tipo de máquina virtual (`class`) y los recursos de almacenamiento asignados a cada nodo (`storageClass`).

Tabla 13-4. Parámetros para aprovisionar clústeres de Tanzu Kubernetes (continuación)

Nombre	Valor	Descripción
`count`	Un entero entre 0 y 150 (por ejemplo, `1`, `2` o `7`)	Especifica la cantidad de nodos de trabajo del clúster. Se puede crear un clúster con cero nodos de trabajo, lo que permite que un clúster solo tenga nodos de plano de control. No hay ningún máximo absoluto para la cantidad de nodos de trabajo, pero 150 es un límite razonable. **Nota** A un clúster aprovisionado con 0 nodos de trabajo no se le asigna ningún servicio de equilibrador de carga.
`class`	Un elemento definido por el sistema en forma de cadena de un conjunto enumerado (por ejemplo, `guaranteed-small` o `best-effort-large`)	Especifica el nombre del elemento VirtualMachineClass que describe la configuración de hardware virtual que se utilizará en cada nodo del grupo. Esto controla el hardware disponible para el nodo (CPU y memoria), así como las solicitudes y los límites de dichos recursos. Consulte Clases de máquina virtual para clústeres de Tanzu Kubernetes.
`storageClass`	`node-storage` (por ejemplo)	Identifica la clase de almacenamiento que se utilizará para almacenar los discos que contienen los sistemas de archivos raíz de los nodos de trabajo. Ejecute `kubectl describe ns` en el espacio de nombres para enumerar las clases de almacenamiento disponibles. Las clases de almacenamiento disponibles para el espacio de nombres varían según el almacenamiento que establece el administrador de vSphere. Las clases de almacenamiento asociadas con el espacio de nombres de supervisor se replican en el clúster. En otras palabras, la clase de almacenamiento debe estar disponible en el espacio de nombres de supervisor para que sea válida. Consulte Capítulo 7 Configurar y administrar los espacios de nombres de vSphere.

Tabla 13-4. Parámetros para aprovisionar clústeres de Tanzu Kubernetes (continuación)

Nombre	Valor	Descripción
`volumes`	Configuración de almacenamiento opcional ■ volúmenes: 　■ nombre: *string* 　■ mountPath: */dir/path* 　■ capacidad 　　■ almacenamiento: tamaño de GiB	Puede especificar parámetros de almacenamiento y disco independientes para las imágenes de contenedor en los nodos de trabajo. Consulte el ejemplo Clúster con discos y parámetros de almacenamiento independientes.
`settings`	Sección para la configuración específica del clúster; todas las `spec.settings` son opcionales	Identifica la información de configuración de tiempo de ejecución opcional del clúster, incluidos los detalles de la instancia de `network` del nodo y la instancia persistente de `storage` de los pods.
`storage`	Sección para especificar almacenamiento	Identifica las entradas de almacenamiento de volumen persistente (Persistent Volume, PV) para las cargas de trabajo de contenedor.
`classes`	Una matriz de una o varias cadenas definidas por el usuario (por ejemplo, `["gold", "silver"]`)	Especifica clases de almacenamiento de volumen persistente (Persistent Volume, PV) con nombre para las cargas de trabajo de contenedor. Las clases de almacenamiento asociadas con el espacio de nombres de supervisor se replican en el clúster. En otras palabras, la clase de almacenamiento debe estar disponible en el espacio de nombres de supervisor para que sea un valor válido. Consulte el ejemplo Clúster con clases de almacenamiento y una clase predeterminada para volúmenes persistentes.

Tabla 13-4. Parámetros para aprovisionar clústeres de Tanzu Kubernetes (continuación)

Nombre	Valor	Descripción
`defaultClass`	`silver` (por ejemplo)	Especifica una clase de almacenamiento con nombre que se anotará como valor predeterminado en el clúster. Si no la especifica, no habrá ningún valor predeterminado. No se tienen que especificar una o varias instancias de `classes` para especificar una instancia de `defaultClass`. Es posible que algunas cargas de trabajo requieran una clase predeterminada, como Helm. Consulte el ejemplo Clúster con clases de almacenamiento y una clase predeterminada para volúmenes persistentes.
`network`	Marcador de sección para la configuración de redes	Especifica la configuración relacionada con la red del clúster.
`cni`	Marcador de sección para especificar la CNI	Identifica el complemento de interfaz de redes del contenedor (Container Networking Interface, CNI) del clúster. El valor predeterminado es Antrea, por lo que no es necesario especificarlo en los clústeres nuevos.
`name`	Cadena `antrea` o `calico`	Especifica la CNI que se utilizará. Las posibles opciones son Antrea y Calico. La configuración del sistema establece Antrea como la CNI predeterminada. El valor predeterminado de la CNI se puede cambiar. Si utiliza el valor predeterminado, no necesita especificar este campo.
`services`	Marcador de sección para especificar subredes de servicios de Kubernetes	Identifica la configuración de red de los servicios de Kubernetes. El valor predeterminado es 10.96.0.0/12.

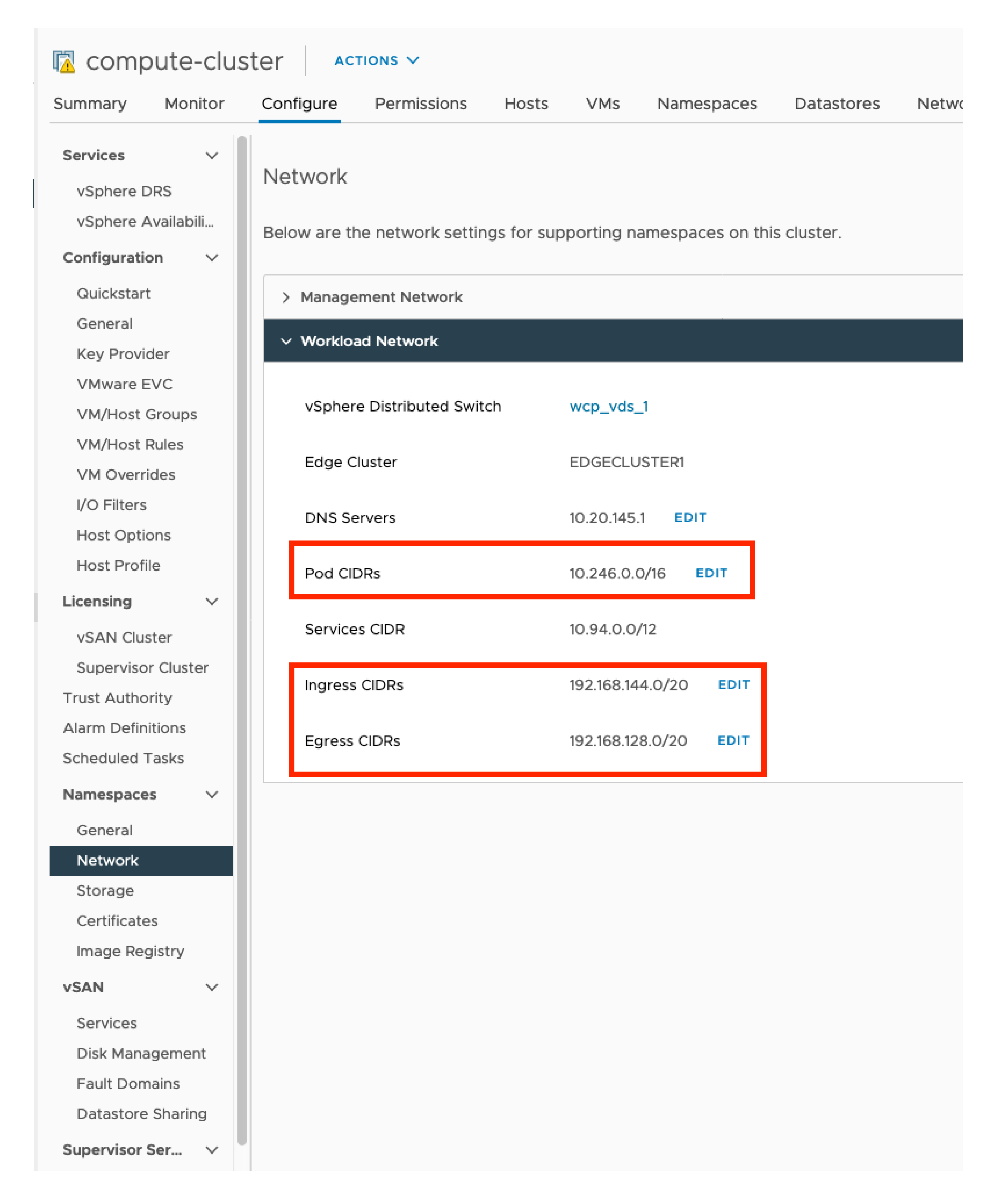
Tabla 13-4. Parámetros para aprovisionar clústeres de Tanzu Kubernetes (continuación)

Nombre	Valor	Descripción
`cidrBlocks`	Matriz `["198.51.100.0/12"]` (por ejemplo)	Especifica un rango de direcciones IP que se puede usar para los servicios de Kubernetes. El valor predeterminado es 10.96.0.0/12. No debe superponerse con la configuración elegida para el clúster supervisor. A pesar de que este campo es una matriz que permite varios rangos, de momento solo se permite un rango de IP único. Consulte los ejemplos de redes en Ejemplos del aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1.
`pods`	Marcador de sección para especificar subredes de pods de Kubernetes	Especifica la configuración de red de los pods. El valor predeterminado es 192.168.0.0/16. El tamaño mínimo de bloque es /24.
`cidrBlocks`	Matriz `["192.0.2.0/16"]` (por ejemplo)	Especifica un rango de direcciones IP que se puede usar para los pods de Kubernetes. El valor predeterminado es 192.168.0.0/16. No debe superponerse con la configuración elegida para el clúster supervisor. El tamaño de la subred de pods debe ser igual o mayor que/24. A pesar de que este campo es una matriz que permite varios rangos, de momento solo se permite un rango de IP único. Consulte los ejemplos de redes en Ejemplos del aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1.
`serviceDomain`	`"cluster.local"`	Especifica el dominio de servicio del clúster. El valor predeterminado es `cluster.local`.
`proxy`	Sección que especifica la configuración de proxy HTTP(s) para el clúster. Si se implementa, todos los campos son obligatorios.	Proporciona campos para la configuración del proxy especificado; se rellenará automáticamente si se configura un proxy global y no se configura un proxy de clúster individual. Consulte el ejemplo Clúster con un servidor proxy.
`httpProxy`	`http://<user>:<pwd>@<ip>:<port>`	Especifica una URL de proxy que se utilizará para crear conexiones HTTP fuera del clúster.

Tabla 13-4. Parámetros para aprovisionar clústeres de Tanzu Kubernetes (continuación)

Nombre	Valor	Descripción
`httpsProxy`	`http://<user>:<pwd>@<ip>:<port>`	Especifica una URL de proxy que se utilizará para crear conexiones HTTPS fuera del clúster.
`noProxy`	Matriz de bloques CIDR que no utilizarán proxy, por ejemplo: `[10.246.0.0/16,192.168.144.0/20,192.168.128.0/20]`. Obtenga los valores necesarios de la red de carga de trabajo en el clúster supervisor: `Pod CIDRs`, `Ingress CIDRs` y `Egress CIDRs`. Consulte la imagen a continuación para ver los valores que se deben incluir en el campo de matriz `noProxy`.	No debe utilizar proxy con las subredes utilizadas por la red de carga de trabajo en el clúster supervisor para pods, entrada y salida. No es necesario incluir el CIDR de servicios del clúster supervisor en el campo `noProxy`. Los clústeres de Tanzu Kubernetes no interactúan con dichos servicios. Los endpoints `localhost` y `127.0.0.1` automáticamente no se usan como proxy. No es necesario que los agregue al campo `noProxy`. Los CIDR de pod y de servicio para los clústeres de Tanzu Kubernetes no se usan como proxy automáticamente. No es necesario que los agregue al campo `noProxy`. Consulte el ejemplo Clúster con un servidor proxy.
`trust`	Marcador de sección para los parámetros de `trust`.	No acepta datos.
`additionalTrustedCAs`	Acepta una matriz de certificados con `name` y `data` para cada uno.	No acepta datos.
`name`	Cadena	El nombre del certificado de TLS.
`data`	Cadena	La cadena codificada en base64 de un certificado público con codificación PEM.

Obtenga los valores de `noProxy` requeridos de la **red de carga de trabajo** del clúster supervisor como se muestra en la imagen.



Ejemplos del aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1

La API de servicio Tanzu Kubernetes Grid proporciona valores predeterminados inteligentes y una gama de opciones para personalizar clústeres de Tanzu Kubernetes. Consulte los ejemplos para

aprovisionar clústeres de varios tipos con configuraciones y personalizaciones diferentes para satisfacer sus necesidades.

YAML mínimo para el aprovisionamiento de un clúster de Tanzu Kubernetes

El siguiente ejemplo de YAML es la configuración mínima necesaria para invocar servicio Tanzu Kubernetes Grid y aprovisionar un clúster de Tanzu Kubernetes que utiliza todas las opciones de configuración predeterminadas.

Las características del YAML mínimo de ejemplo incluyen:

- La versión de versión de Tanzu Kubernetes, que aparece como v1.19, se resolverá en la distribución más reciente que coincida con esa versión secundaria, por ejemplo, `v1.19.7+vmware.1-tkg.1.xxxxxx`. Consulte Comprobar la compatibilidad del clúster de Tanzu Kubernetes para actualizar.
- La clase de máquina virtual `best-effort-<size>` no tiene reservas. Para obtener más información, consulte Clases de máquina virtual para clústeres de Tanzu Kubernetes.
- El clúster no incluye almacenamiento persistente para los contenedores. Si es necesario, se establece en `spec.settings.storage`. Consulte el ejemplo de almacenamiento a continuación.
- Es posible que algunas cargas de trabajo, como Helm, requieran una `spec.settings.storage.defaultClass`. Consulte el ejemplo de almacenamiento a continuación.
- No se especificó la sección `spec.settings.network`. Esto significa que el clúster utiliza la siguiente configuración de red predeterminada:
  - CNI predeterminada: `antrea`
  - CIDR de pod predeterminado: `192.168.0.0/16`
  - CIDR de servicios predeterminados: `10.96.0.0/12`
  - Dominio de servicio predeterminado: `cluster.local`

Nota El rango de IP predeterminado para los pods es `192.168.0.0/16`. Si esta subred ya está en uso, debe especificar un rango de CIDR diferente. Consulte los ejemplos de redes personalizadas que aparecen a continuación.

```
apiVersion: run.tanzu.vmware.com/v1alpha1      #TKGS API endpoint
kind: TanzuKubernetesCluster                   #required parameter
metadata:
  name: tkgs-cluster-1                         #cluster name, user defined
  namespace: tgks-cluster-ns                   #vsphere namespace
spec:
  distribution:
    version: v1.20                             #Resolves to latest TKR 1.20
  topology:
    controlPlane:
      count: 1                                 #number of control plane nodes
```

```
      class: best-effort-medium                #vmclass for control plane nodes
      storageClass: vwt-storage-policy         #storageclass for control plane
    workers:
      count: 3                                 #number of worker nodes
      class: best-effort-medium                #vmclass for worker nodes
      storageClass: vwt-storage-policy         #storageclass for worker nodes
```

Clúster con discos y parámetros de almacenamiento independientes

En el siguiente ejemplo de YAML se muestra cómo aprovisionar un clúster con discos y parámetros de almacenamiento independientes para los nodos de trabajo y el plano de control del clúster.

Al usar discos y parámetros de almacenamiento independientes para los datos de renovación alta, se minimiza la sobrecarga de lectura-escritura relacionada con el uso de los clones vinculados, entre otras ventajas. Existen dos casos prácticos principales:

- Personalizar el rendimiento del almacenamiento en nodos del plano de control para la base de datos de etcd
- Personalizar el tamaño del disco para las imágenes de contenedor en los nodos de trabajo

El ejemplo tiene las siguientes características:

- La configuración de `spec.topology.controlPlane.volumes` especifica el volumen independiente para la base de datos de etcd.
- La configuración de `spec.topology.workers.volumes` especifica el volumen independiente para las imágenes de contenedor.
- `mountPath: /var/lib/containerd` para las imágenes de contenedor es compatible con las versiones 1.17 de Tanzu Kubernetes y otras posteriores.

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TanzuKubernetesCluster
metadata:
  name: tkgs-cluster-5
  namespace: tgks-cluster-ns
spec:
  distribution:
    version: v1.20
  topology:
    controlPlane:
      count: 3
      class: best-effort-medium
      storageClass: vwt-storage-policy
      volumes:
        - name: etcd
          mountPath: /var/lib/etcd
          capacity:
            storage: 4Gi
    workers:
      count: 3
```

```
      class: best-effort-medium
      storageClass: vwt-storage-policy
      volumes:
        - name: containerd
          mountPath: /var/lib/containerd
          capacity:
            storage: 16Gi
```

Clúster con una red Antrea personalizada

En el siguiente YAML se muestra cómo aprovisionar un clúster de Tanzu Kubernetes con rangos de redes personalizadas para la CNI de Antrea.

- Debido a que se aplica la configuración de red personalizada, se requiere el parámetro `cni.name` aunque se utilice la CNI de Antrea predeterminada.
  - Nombre de CNI: `antrea`
  - CIDR de pods personalizados: `193.0.2.0/16`
  - CIDR de servicios personalizados: `195.51.100.0/12`
  - Dominio de servicio personalizado: `managedcluster.local`
- Los bloques CIDR personalizados no pueden superponerse con el clúster supervisor. Para obtener más información, consulte Parámetros de configuración para clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1.

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TanzuKubernetesCluster
metadata:
  name: tkg-cluster-3-antrea
  namespace: tkgs-cluster-ns
spec:
  distribution:
    version: v1.20
  topology:
    controlPlane:
      class: guaranteed-medium
      count: 3
      storageClass: vwt-storage-policy
    workers:
      class: guaranteed-medium
      count: 5
      storageClass: vwt-storage-policy
  settings:
    network:
      cni:
        name: antrea                       #Use Antrea CNI
      pods:
        cidrBlocks:
        - 193.0.2.0/16                     #Must not overlap with SVC
```

```
      services:
        cidrBlocks:
        - 195.51.100.0/12                  #Must not overlap with SVC
      serviceDomain: managedcluster.local
```

Clúster con una red Calico personalizada

El siguiente YAML demuestra cómo aprovisionar un clúster de Tanzu Kubernetes con una red Calico personalizada.

- Calico no es la CNI predeterminada, por lo que se nombra de forma explícita en el manifiesto. Para cambiar la CNI predeterminada en el nivel de servicio, consulte Ejemplos de configuración de la API de servicio Tanzu Kubernetes Grid v1alpha1.
  - Nombre de CNI: `calico`
  - CIDR de pods personalizados: `198.51.100.0/12`
  - CIDR de servicios personalizados: `192.0.2.0/16`
  - Dominio de servicio personalizado: `managedcluster.local`
- La red utiliza rangos de CIDR personalizados, y no los predeterminados. Estos rangos no deben superponerse con el clúster supervisor. Consulte Parámetros de configuración para clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1.

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TanzuKubernetesCluster
metadata:
  name: tkgs-cluster-2
  namespace: tkgs-cluster-ns
spec:
  distribution:
    version: v1.20
  topology:
    controlPlane:
      count: 3
      class: guaranteed-large
      storageClass: vwt-storage-policy
    workers:
      count: 5
      class: guaranteed-xlarge
      storageClass: vwt-storage-policy
  settings:
    network:
      cni:
        name: calico                          #Use Calico CNI for this cluster
      services:
        cidrBlocks: ["198.51.100.0/12"]       #Must not overlap with SVC
      pods:
        cidrBlocks: ["192.0.2.0/16"]          #Must not overlap with SVC
      serviceDomain: managedcluster.local
```

Clúster con clases de almacenamiento y una clase predeterminada para volúmenes persistentes

El siguiente ejemplo de YAML demuestra cómo aprovisionar un clúster con clases de almacenamiento para el aprovisionamiento dinámico de PVC y una clase de almacenamiento predeterminada.

- La opción `spec.settings.storage.classes` especifica dos clases de almacenamiento para el almacenamiento persistente de los contenedores en el clúster.
- Se especifica `spec.settings.storage.defaultClass`. Algunas aplicaciones requieren una clase predeterminada. Por ejemplo, si desea utilizar Helm o Kubeapps como la `defaultClass` a la que hacen referencia muchos gráficos.

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TanzuKubernetesCluster
metadata:
  name: default-storage-spec
  namespace: tkgs-cluster-ns
spec:
  topology:
    controlPlane:
      count: 3
      class: best-effort-medium
      storageClass: vwt-storage-policy
    workers:
      count: 3
      class: best-effort-medium
      storageClass: vwt-storage-policy
  distribution:
    version: v1.20
  settings:
    network:
      cni:
        name: antrea
      services:
        cidrBlocks: ["198.51.100.0/12"]
      pods:
        cidrBlocks: ["192.0.2.0/16"]
      serviceDomain: "tanzukubernetescluster.local"
    storage:
      classes: ["gold", "silver"]              #Array of named PVC storage classes
      defaultClass: silver                     #Default PVC storage class
```

Clúster con un servidor proxy

Puede utilizar un servidor proxy con un clúster de Tanzu Kubernetes individual si se aplica la configuración del servidor proxy al manifiesto del clúster.

Tenga en cuenta las siguientes características:

- La sección `spec.settings.network.proxy` especifica la configuración del proxy HTTP(s) para este clúster de Tanzu Kubernetes.

- La sintaxis de ambos valores del servidor `proxy` es `http://<user>:<pwd>@<ip>:<port>`.
- Los endpoints específicos no se convierten automáticamente en proxy, incluidos `localhost` y `127.0.0.1`, y los CIDR de pod y de servicio para clústeres de Tanzu Kubernetes. No es necesario incluirlos en el campo `noProxy`.
- El campo `noProxy` acepta una matriz de CIDR para que no sea proxy. Obtenga los valores necesarios de la red de carga de trabajo del clúster supervisor. Consulte la imagen en Parámetros de configuración para clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1.
- Si se configura un proxy global en `TkgServiceConfiguration`, esa información de proxy se propaga al manifiesto del clúster después de la implementación inicial del clúster. La configuración global del proxy se agrega al manifiesto del clúster solo si no hay ningún campo de configuración de proxy presente cuando se crea el clúster. En otras palabras, la configuración por clúster tiene prioridad y sobrescribirá la configuración global del proxy.

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TanzuKubernetesCluster
metadata:
  name: tkgs-cluster-with-proxy
  namespace: tkgs-cluster-ns
spec:
  distribution:
    version: v1.20
  topology:
    controlPlane:
      count: 3
      class: guaranteed-medium
      storageClass: vwt-storage-policy
    workers:
      count: 5
      class: guaranteed-xlarge
      storageClass: vwt-storage-policy
  settings:
    storage:
      classes: ["gold", "silver"]
      defaultClass: silver
    network:
      cni:
        name: antrea
      pods:
        cidrBlocks:
        - 193.0.2.0/16
      services:
        cidrBlocks:
        - 195.51.100.0/12
      serviceDomain: managedcluster.local
      proxy:
        httpProxy: http://10.186.102.224:3128  #Proxy URL for HTTP connections
        httpsProxy: http://10.186.102.224:3128 #Proxy URL for HTTPS connections
```

```
        noProxy: [10.246.0.0/16,192.168.144.0/20,192.168.128.0/20] #SVC Pod, Egress, Ingress 
CIDRs
```

Clúster con certificados personalizados para TLS

De forma similar a cómo puede especificar `trust.additionalTrustedCAs` en `TkgServiceConfiguration` (consulte Parámetros de configuración para la API v1alpha1 de servicio Tanzu Kubernetes Grid), puede incluir `trust.additionalTrustedCAs` en `spec.settings.network` en la especificación del `TanzuKubernetesCluster`. Por ejemplo:

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TanzuKubernetesCluster
metadata:
  name: tkgs-cluster-with-custom-certs-tls
  namespace: tkgs-cluster-ns
spec:
  topology:
    controlPlane:
      count: 3
      class: guaranteed-medium
      storageClass: vwt-storage-profile
    workers:
      count: 3
      class: guaranteed-large
      storageClass: vwt-storage-profile
  distribution:
    version: 1.20.2
  settings:
    network:
      cni:
        name: antrea
      services:
        cidrBlocks: ["198.51.100.0/12"]
      pods:
        cidrBlocks: ["192.0.2.0/16"]
      serviceDomain: "managedcluster.local"
      trust:
        additionalTrustedCAs:
          - name: custom-selfsigned-cert-for-tkc
            data: |
              LS0aaaaaaaaaaaaaaabase64...
```

El clúster que hereda o no la configuración global de la especificación TkgServiceConfiguration

Nota Las siguientes configuraciones de clúster de ejemplo requieren la versión 7.0U2a de vCenter Server y otras versiones posteriores y, al menos, la versión 1.18.10 de clúster supervisor.

Para aprovisionar un clúster de Tanzu Kubernetes que hereda una configuración global de la `TkgServiceConfiguration`, configure el clúster con la configuración global no especificada o anulada.

Por ejemplo, si desea configurar un clúster que herede la configuración del `proxy`, podría utilizar cualquiera de los siguientes métodos:

Opción 1: Incluir la configuración del `proxy` en la especificación del clúster:

```
...
settings:
  network:
    cni:
      name: antrea
    services:
      cidrBlocks: ["198.51.100.0/12"]
    pods:
      cidrBlocks: ["192.0.2.0/16"]
    serviceDomain: "tanzukubernetescluster.local"
```

Opción 2: Incluir la configuración del `proxy` en la especificación, pero establecer explícitamente su valor en `null`:

```
settings:
  network:
    proxy: null
```

Para aprovisionar un clúster de Tanzu Kubernetes que no herede el valor predeterminado de la `TkgServiceConfiguration`, configure la especificación del clúster con todos los elementos incluidos pero vacíos.

Por ejemplo, si la `TkgServiceConfiguration` tiene un `proxy` global configurado y desea aprovisionar un clúster que no herede la configuración global del `proxy`, incluya la siguiente sintaxis en la especificación del clúster:

```
...
settings:
  network:
    proxy:
      httpProxy: ""
      httpsProxy: ""
      noProxy: null
```

Clúster que utiliza una biblioteca de contenido local

Para aprovisionar un clúster de Tanzu Kubernetes en un entorno aislado, cree un clúster con la imagen de máquina virtual sincronizada desde una biblioteca de contenido local.

Para aprovisionar un clúster con una imagen de la biblioteca de contenido local, debe introducir esa imagen en la especificación del clúster. Para el valor `distribution.version`, puede introducir el nombre completo de la imagen o, si ha mantenido el formato de nombre del directorio de la imagen, puede acortarlo a la versión de Kubernetes. Si desea utilizar un número de versión completo, reemplace `-----` por `+`. Por ejemplo, si tiene una imagen OVA llamada `photon-3-k8s-v1.20.2---vmware.1-tkg.1.1d4f79a`, se aceptan los siguientes formatos.

```
spec:
  distribution:
    version: v1.20
```

```
spec:
  distribution:
    version: v1.20.2
```

```
spec:
  distribution:
    version: v1.20.2+vmware.1-tkg.1
```

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TanzuKubernetesCluster
metadata:
    name: tgks-cluster-9
    namespace: tkgs-cluster-ns
spec:
   topology:
       controlPlane:
           count: 3
           class: best-effort-medium
           storageClass: vwt-storage-policy
       workers:
           count: 3
           class: best-effort-medium
           storageClass: vwt-storage-policy
   distribution:
        version: v1.20.2
   settings:
        network:
          cni:
              name: antrea
          services:
             cidrBlocks: ["198.51.100.0/12"]
          pods:
             cidrBlocks: ["192.0.2.0/16"]
```

Parámetros de configuración para la API v1alpha1 de servicio Tanzu Kubernetes Grid

Puede personalizar servicio Tanzu Kubernetes Grid con ajustes globales de funciones clave, como la interfaz de redes de contenedor (Container Network Interface, CNI), el servidor proxy y los certificados TLS. Tenga presentes las consideraciones y las concesiones necesarias al implementar la funcionalidad global frente a la funcionalidad por clúster.

De forma opcional, puede configurar servicio Tanzu Kubernetes Grid con parámetros globales.

Precaución La configuración de servicio Tanzu Kubernetes Grid es una operación global. Esto significa que cualquier cambio que realice en la especificación `TkgServiceConfiguration` se aplicará a todos los clústeres de Tanzu Kubernetes aprovisionados por ese servicio. Si se inicia una actualización gradual, ya sea de forma manual o mediante actualización, los clústeres se actualizan según la especificación de servicio modificada.

Especificación TkgServiceConfiguration

La especificación `TkgServiceConfiguration` proporciona campos para configurar la instancia de servicio Tanzu Kubernetes Grid.

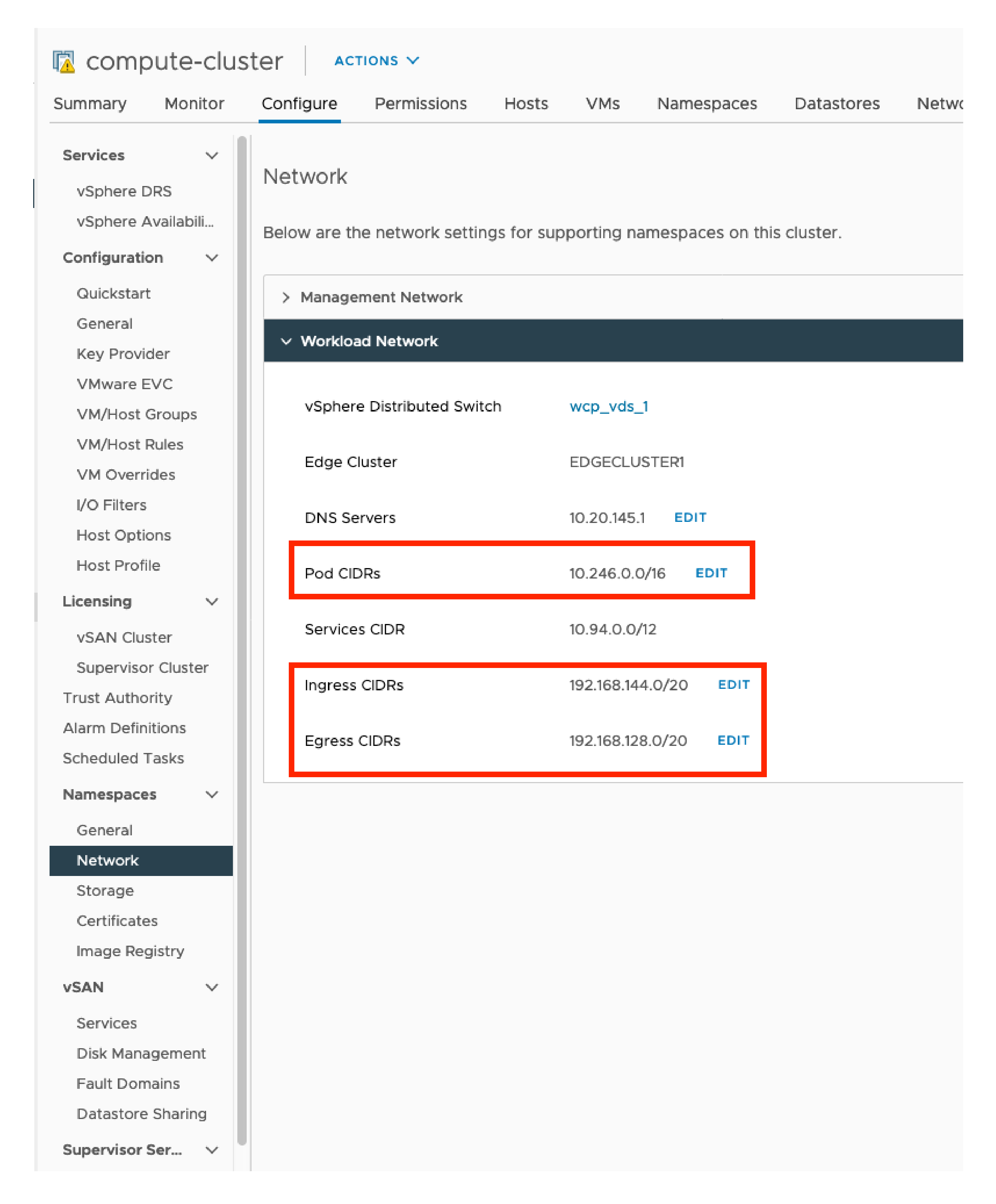
```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TkgServiceConfiguration
metadata:
  name: tkg-service-configuration-example
spec:
  defaultCNI: <antrea or calico>
  proxy:
    httpProxy: http://<user>:<pwd>@<ip>:<port>
    httpsProxy: http://<user>:<pwd>@<ip>:<port>
    noProxy: [<array of CIDRs to not proxy>]
  trust:
    additionalTrustedCAs:
      - name: <first-cert-name>
        data: <base64-encoded string of a PEM encoded public cert 1>
      - name: <second-cert-name>
        data: <base64-encoded string of a PEM encoded public cert 2>
```

Parámetros de la especificación TcardServiceConfiguration

En la tabla se enumeran y describen cada uno de los parámetros de la especificación `TkgServiceConfiguration`. Para ver ejemplos, consulte Ejemplos de configuración de la API de servicio Tanzu Kubernetes Grid v1alpha1.

Campo	Valor	Descripción
defaultCNI	antrea or calico	CNI predeterminada para que utilicen los clústeres. El valor predeterminado es antrea. La otra CNI admitida es calico.
proxy	Marcador de sección para los parámetros de proxy.	Los parámetros de proxy son httpProxy, httpsProxy y noProxy. Todos los parámetros son obligatorios. Si falta algún parámetro de proxy, no podrá crear clústeres de Tanzu Kubernetes.
httpProxy	URI con el formato http://<user>:<pwd>@<ip>:<port>	No permite el protocolo https. Si se utiliza https, no se podrán crear clústeres de Tanzu Kubernetes.
httpsProxy	URI con el formato http://<user>:<pwd>@<ip>:<port>	No permite el protocolo https. Si se utiliza https, no se podrán crear clústeres de Tanzu Kubernetes.
noProxy	Matriz de bloques CIDR que no utilizarán proxy, por ejemplo: [10.246.0.0/16,192.168.144.0/20,192.168.128.0/20]. Obtenga los valores necesarios de la red de carga de trabajo en el clúster supervisor: Pod CIDRs, Ingress CIDRs y Egress CIDRs. Consulte la imagen a continuación para ver los valores que se deben incluir en el campo de matriz noProxy.	No debe utilizar proxy con las subredes utilizadas por la red de carga de trabajo en el clúster supervisor para pods, entrada y salida. No es necesario incluir el CIDR de servicios del clúster supervisor en el campo noProxy. Los clústeres de Tanzu Kubernetes no interactúan con dichos servicios. Los endpoints localhost y 127.0.0.1 automáticamente no se usan como proxy. No es necesario que los agregue al campo noProxy. Los CIDR de pod y de servicio para los clústeres de Tanzu Kubernetes no se usan como proxy automáticamente. No es necesario que los agregue al campo noProxy.
trust	Marcador de sección para los parámetros de trust.	No acepta datos.
additionalTrustedCAs	Acepta una matriz de certificados con name y data para cada uno.	No acepta datos.
name	Cadena	El nombre del certificado de TLS.
data	Cadena	La cadena codificada en base64 de un certificado público con codificación PEM.

Obtenga los valores de noProxy requeridos de la **red de carga de trabajo** del clúster supervisor como se muestra en la imagen.



Cuándo utilizar las opciones de configuración globales o por clúster

`TkgServiceConfiguration` es una especificación global que afecta a todos los clústeres de Tanzu Kubernetes aprovisionados por la instancia de servicio Tanzu Kubernetes Grid.

Antes de editar `TkgServiceConfiguration`, tenga en cuenta las alternativas por clúster que pueden satisfacer su caso práctico, en lugar de una configuración global.

Tabla 13-5. Opciones de configuración global frente a opciones por clúster

Configuración	Opción global	Opción por clúster
CNI predeterminada	Edite la especificación `TkgServiceConfiguration`. Consulte Ejemplos de configuración de la API de servicio Tanzu Kubernetes Grid v1alpha1.	Especifique la CNI en la especificación del clúster. Por ejemplo, Antrea es la CNI predeterminada. Para usar Calico, especifíquelo en el YAML del clúster. Consulte Ejemplos del aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1.
Servidor proxy	Edite la especificación `TkgServiceConfiguration`. Consulte Ejemplos de configuración de la API de servicio Tanzu Kubernetes Grid v1alpha1.	Incluya los parámetros de configuración del servidor proxy en la especificación del clúster. Consulte Ejemplos del aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1.
Certificados de confianza	Edite la especificación `TkgServiceConfiguration`. Existen dos casos de uso: configurar un registro de contenedor externo y una configuración de proxy basada en certificados. Consulte Ejemplos de configuración de la API de servicio Tanzu Kubernetes Grid v1alpha1.	Sí, puede incluir certificados personalizados por clúster o anular la configuración de `trust` establecida globalmente en la especificación del clúster. Consulte Ejemplos del aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1.

Nota Si se configura un proxy global en `TkgServiceConfiguration`, esa información de proxy se propaga al manifiesto del clúster después de la implementación inicial del clúster. La configuración global del proxy se agrega al manifiesto del clúster solo si no hay ningún campo de configuración de proxy presente cuando se crea el clúster. En otras palabras, la configuración por clúster tiene prioridad y sobrescribirá la configuración global del proxy. Para obtener más información, consulte Parámetros de configuración para la API v1alpha1 de servicio Tanzu Kubernetes Grid.

Antes de editar la especificación `TkgServiceConfiguration`, tenga en cuenta las ramificaciones de aplicar la configuración a nivel global.

Campo	Se aplica	Impacto en los clústeres existentes si se agrega o se cambia	Anulación por clúster al crear un clúster	Anulación por clúster al actualizar un clúster
`defaultCNI`	Globalmente	Ninguno	Sí, puede anular la configuración global al crear el clúster	No, no puede cambiar la CNI de un clúster existente. Si utilizó la CNI predeterminada configurada globalmente al crear el clúster, no puede cambiarla
`proxy`	Globalmente	Ninguno	Sí, puede anular la configuración global al crear el clúster	Sí, con U2+ puede anular la configuración global al actualizar el clúster
`trust`	Globalmente	Ninguno	Sí, puede anular la configuración global al crear el clúster	Sí, con U2+ puede anular la configuración global al actualizar el clúster

Propagar cambios de configuración global a clústeres existentes

La configuración realizada a nivel global en `TkgServiceConfiguration` no se propaga automáticamente a los clústeres existentes. Por ejemplo, si realiza cambios en la configuración de `proxy` o `trust` en `TkgServiceConfiguration`, dichos cambios no afectarán a los clústeres que ya están aprovisionados.

Para propagar un cambio global a un clúster existente, debe aplicar una revisión al clúster de Tanzu Kubernetes para que herede los cambios realizados en `TkgServiceConfiguration`.

Por ejemplo:

```
kubectl patch tkc <CLUSTER_NAME> -n <NAMESPACE> --type merge -p "{\"spec\":{\"settings\":
{\"network\":{\"proxy\": null}}}}"
```

```
kubectl patch tkc <CLUSTER_NAME> -n <NAMESPACE> --type merge -p "{\"spec\":{\"settings\":
{\"network\":{\"trust\": null}}}}"
```

Ejemplos de configuración de la API de servicio Tanzu Kubernetes Grid v1alpha1

Consulte los ejemplos para personalizar servicio Tanzu Kubernetes Grid con opciones de configuración global para la interfaz de redes de contenedor (Container Network Interface, CNI), el servidor proxy y los certificados TLS.

Acerca de la configuración de servicio Tanzu Kubernetes Grid

Para personalizar servicio Tanzu Kubernetes Grid, cambie la CNI predeterminada, agregue un servidor proxy global y agregue certificados de confianza. Consulte Parámetros de configuración para la API v1alpha1 de servicio Tanzu Kubernetes Grid.

Precaución La edición de la especificación de servicio Tanzu Kubernetes Grid produce cambios globales en todos los clústeres aprovisionados por ese servicio, incluidos los clústeres nuevos y los existentes que se actualizan de forma manual o automática.

Requisito previo: Configurar la edición de Kubectl

Para escalar un clúster de Tanzu Kubernetes, actualice el manifiesto del clúster mediante el comando `kubectl edit tanzukubernetescluster/CLUSTER-NAME`. El comando kubectl edit abre el manifiesto del clúster en el editor de texto definido por las variables de entorno KUBE_EDITOR o EDITOR. Para obtener instrucciones sobre cómo configurar la variable de entorno, consulte Especificar un editor de texto predeterminado para Kubectl.

Al guardar los cambios en la especificación, `kubectl` informa de que las ediciones se registraron correctamente. Para cancelar, simplemente cierre el editor sin guardar.

Configurar la CNI predeterminada

servicio Tanzu Kubernetes Grid proporciona una interfaz de redes de contenedor (Container Network Interface, CNI) predeterminada para los clústeres de Tanzu Kubernetes. La configuración predeterminada permite crear clústeres sin que para ello sea necesario especificar la CNI. Para cambiar el valor de CNI predeterminado, edite la especificación del servicio.

servicio Tanzu Kubernetes Grid admite dos CNI: Antrea y Calico, de las cuales Antrea es la predeterminada. Para obtener más información, consulte Redes de clústeres de servicio Tanzu Kubernetes Grid .

También es posible anular la CNI predeterminada. Para ello, especifique de forma explícita la CNI que se va a utilizar. Como alternativa, puede cambiar la CNI predeterminada mediante la edición del controlador del servicio de TKG para las CNI.

1 Realice la autenticación con clúster supervisor.

```
kubectl vsphere login --server=SVC-IP-ADDRESS --vsphere-username USERNAME
```

2 Cambie el contexto al espacio de nombres de vSphere de destino.

```
kubectl config use-context tkgs-cluster-ns
```

3 Indique la CNI predeterminada.

```
kubectl get tkgserviceconfigurations
```

Resultado de ejemplo:

```
NAME                                  DEFAULT CNI
tkg-service-configuration             antrea
```

4 Cargue para editar la especificación de servicio Tanzu Kubernetes Grid.

```
kubectl edit tkgserviceconfigurations tkg-service-configuration
```

El sistema abre la especificación `tkg-service-configuration` en el editor de texto predeterminado que definen las variables de entorno KUBE_EDITOR o EDITOR.

5 Edite el valor de `spec.defaultCNI`.

Por ejemplo, cambie desde:

```
spec:
  defaultCNI: antrea
```

Cambie a:

```
spec:
  defaultCNI: calico
```

6 Para aplicar los cambios, guarde el archivo en el editor de texto. Para cancelar, cierre el editor sin guardar.

Al guardar el cambio en el editor de texto, kubectl actualiza la especificación de servicio de `tkg-service-configuration`.

7 Compruebe que se haya actualizado la CNI predeterminada.

```
kubectl get tkgserviceconfigurations
```

Se actualiza la CNI predeterminada. Cualquier clúster aprovisionado con la configuración de red predeterminada utiliza la CNI predeterminada.

```
NAME                                  DEFAULT CNI
tkg-service-configuration             calico
```

Configurar un servidor proxy global

Para habilitar un servidor proxy global, agregue los parámetros del servidor proxy a `TkgServiceConfiguration`. Si desea ver una descripción de los campos requeridos, consulte Parámetros de configuración para la API v1alpha1 de servicio Tanzu Kubernetes Grid.

1 Realice la autenticación con clúster supervisor.

```
kubectl vsphere login --server=SVC-IP-ADDRESS --vsphere-username USERNAME
```

2 Cambie el contexto al espacio de nombres de vSphere de destino.

```
kubectl config use-context tkgs-cluster-ns
```

3 Obtener la configuración actual.

```
kubectl get tkgserviceconfigurations
```

Resultado de ejemplo:

```
NAME                          DEFAULT CNI
tkg-service-configuration     antrea
```

4 Cargue para editar la especificación de servicio Tanzu Kubernetes Grid.

```
kubectl edit tkgserviceconfigurations tkg-service-configuration
```

El sistema abre la especificación `tkg-service-configuration` en el editor de texto predeterminado que definen las variables de entorno KUBE_EDITOR o EDITOR.

5 Agregue la subsección `spec.proxy` con cada campo que se pide, incluidos `httpProxy`, `httpsProxy` y `noProxy`.

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TkgServiceConfiguration
metadata:
  ...
  name: tkg-service-configuration-example
  resourceVersion: "44170525"
  selfLink: /apis/run.tanzu.vmware.com/v1alpha1/tkgserviceconfigurations/tkg-service-
configuration
  uid: 10347195-5f0f-490e-8ae1-a758a724c0bc
spec:
  defaultCNI: antrea
  proxy:
    httpProxy: http://<user>:<pwd>@<ip>:<port>
    httpsProxy: http://<user>:<pwd>@<ip>:<port>
    noProxy: [SVC-POD-CIDRs, SVC-EGRESS-CIDRs, SVC-INGRESS-CIDRs]
```

6 Rellene cada campo de proxy con los valores adecuados. Si desea ver una descripción de cada campo, consulte Parámetros de configuración para la API v1alpha1 de servicio Tanzu Kubernetes Grid.

Los valores requeridos para el campo `noProxy` provienen de la **Red de cargas de trabajo** del clúster supervisor. Consulte la imagen en el tema anterior sobre dónde obtener estos valores.

Por ejemplo:

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TkgServiceConfiguration
metadata:
  ...
  name: tkg-service-configuration-example
  resourceVersion: "44170525"
  selfLink: /apis/run.tanzu.vmware.com/v1alpha1/tkgserviceconfigurations/tkg-service-
configuration
  uid: 10347195-5f0f-490e-8ae1-a758a724c0bc
spec:
  defaultCNI: antrea
  proxy:
    httpProxy: http://user:password@10.186.102.224:3128
    httpsProxy: http://user:password@10.186.102.224:3128
    noProxy: [10.246.0.0/16,192.168.144.0/20,192.168.128.0/20]
```

7 Para aplicar los cambios, guarde el archivo en el editor de texto. Para cancelar, cierre el editor sin guardar.

Al guardar los cambios en el editor de texto, kubectl actualiza servicio Tanzu Kubernetes Grid con la configuración definida en la especificación de servicio de `tkg-service-configuration`.

8 Compruebe que el servicio Tanzu Kubernetes Grid se haya actualizado con la configuración del proxy.

```
kubectl get tkgserviceconfigurations -o yaml
```

9 Para comprobarlo, aprovisione el clúster Tanzu Kubernetes. Consulte Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS.

Utilice el siguiente comando para confirmar que el clúster está utilizando el proxy.

```
kubectl get tkc CLUSTER-NAME -n NAMESPACE -o yaml
```

Configuración de un proxy basado en certificados

El uso de un servidor proxy para enrutar el tráfico de Internet es un requisito estricto en algunos entornos. Por ejemplo, una empresa de un sector con muchas regulaciones, como una entidad financiera, requiere que todo el tráfico de Internet pase por un proxy corporativo.

Puede configurar servicio Tanzu Kubernetes Grid para aprovisionar clústeres de Tanzu Kubernetes para que utilicen un servidor proxy para el tráfico HTTP/S saliente. Para obtener más información, consulte Parámetros de configuración para la API v1alpha1 de servicio Tanzu Kubernetes Grid.

Como se muestra en el ejemplo, puede agregar certificados de confianza para el servidor proxy a la especificación `TkgServiceConfiguration`.

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TkgServiceConfiguration
metadata:
  name: tkg-service-configuration-example
spec:
  defaultCNI: antrea
  proxy:
    httpProxy: http://user:password@10.186.102.224:3128
    httpsProxy: http://user:password@10.186.102.224:3128
    noProxy: [10.246.0.0/16,192.168.144.0/20,192.168.128.0/20]
  trust:
    additionalTrustedCAs:
      - name: first-cert-name
        data: base64-encoded string of a PEM encoded public cert 1
      - name: second-cert-name
        data: base64-encoded string of a PEM encoded public cert 2
```

Configuración del registro privado externo

Puede configurar servicio Tanzu Kubernetes Grid con certificados personalizados para conectar clústeres de Tanzu Kubernetes con un registro privado externo. Para obtener más información, consulte Usar un registro de contenedor externo con clústeres de Tanzu Kubernetes.

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TkgServiceConfiguration
metadata:
  name: tkg-service-configuration-example
spec:
  defaultCNI: antrea
  trust:
    additionalTrustedCAs:
      - name: harbor-vm-cert
        data: <<<base64-encoded string of a PEM encoded public cert>>>>
```

Escalar un clúster de Tanzu Kubernetes mediante la API v1alpha1 de servicio Tanzu Kubernetes Grid

Puede ampliar un clúster de Tanzu Kubernetes horizontalmente cambiando el número de nodos o verticalmente, cambiando la clase de máquina virtual que aloja los nodos.

Operaciones de ampliación admitidas

En la tabla se enumeran las operaciones de ampliación admitidas para clústeres de Tanzu Kubernetes.

Tabla 13-6. Operaciones de ampliación admitidas para clústeres de Tanzu Kubernetes

Nodo	Expansión horizontal	Reducción horizontal	Ampliación vertical
Plano de control	Sí	No	Sí
Trabajador	Sí	Sí	Sí

Tenga en cuenta las siguientes consideraciones:

- Al ampliar verticalmente un nodo de clúster, es posible que las cargas de trabajo ya no puedan ejecutarse en el nodo por falta de recursos disponibles. Por esta razón, puede que la ampliación horizontal sea el método preferido.
- Las clases de máquina virtual no son inmutables. Si se escala horizontalmente un clúster de Tanzu Kubernetes después de editar una clase de máquina virtual utilizada por ese clúster, los nuevos nodos del clúster utilizan la definición de clase actualizada, pero los nodos del clúster existentes siguen usando la definición de clase inicial, lo que provoca un error de coincidencia. Consulte Clases de máquina virtual para clústeres de Tanzu Kubernetes.

Requisito previo para la ampliación: configurar la edición de Kubectl

Para escalar un clúster de Tanzu Kubernetes, actualice el manifiesto del clúster mediante el comando `kubectl edit tanzukubernetescluster/CLUSTER-NAME`. El comando kubectl edit abre el manifiesto del clúster en el editor de texto definido por las variables de entorno KUBE_EDITOR o EDITOR. Para obtener instrucciones sobre cómo configurar la variable de entorno, consulte Especificar un editor de texto predeterminado para Kubectl.

Al guardar los cambios del manifiesto, `kubectl` informa que las modificaciones se registraron correctamente, y el clúster se actualiza con los cambios.

```
kubectl edit tanzukubernetescluster/tkgs-cluster-1
tanzukubernetescluster.run.tanzu.vmware.com/tkgs-cluster-1 edited
```

Para cancelar, simplemente cierre el editor sin guardar.

```
kubectl edit tanzukubernetescluster/tkgs-cluster-1
Edit cancelled, no changes made.
```

Ampliar horizontalmente el plano de control

Para ampliar horizontalmente un clúster de Tanzu Kubernetes, aumente el número de nodos del plano de control de 1 a 3. El número de nodos del plano de control debe ser impar. No se puede realizar una ampliación vertical en el plano de control.

1 Realice la autenticación con clúster supervisor.

```
kubectl vsphere login --server=SVC-IP-ADDRESS --vsphere-username USERNAME
```

2 Cambie el contexto al espacio de nombres de vSphere en el que se aprovisiona el clúster de Tanzu Kubernetes.

```
kubectl config use-context tkgs-cluster-ns
```

3 Enumere los clústeres de Kubernetes que se están ejecutando en el espacio de nombres.

```
kubectl get tanzukubernetescluster -n tkgs-cluster-ns
```

4 Obtenga la cantidad de nodos que se ejecutan en el clúster de destino.

```
kubectl get tanzukubernetescluster tkgs-cluster-1
```

Por ejemplo, el siguiente clúster tiene 1 nodo de plano de control y 3 nodos de trabajo.

```
NAME                CONTROL PLANE   WORKER   DISTRIBUTION                       AGE   PHASE
tkgs-cluster-1      1               3        v1.18.5+vmware.1-tkg.1.886c781     1d    running
```

5 Cargue el manifiesto del clúster para editarlo ejecutando el comando `kubectl edit`.

```
kubectl edit tanzukubernetescluster/tkgs-cluster-1
```

El manifiesto del clúster se abrirá en el editor de texto que definan las variables de entorno KUBE_EDITOR o EDITOR.

6 Busque el parámetro `spec.topology.controlPlane.count` y aumente el número de nodos de 1 a 3.

```
...
controlPlane:
    count: 1
...
```

```
...
ControlPlane:
    count: 3
...
```

7 Para aplicar los cambios, guarde el archivo en el editor de texto. Para cancelar, cierre el editor sin guardar.

Cuando guarde el archivo, kubectl aplicará los cambios al clúster. En segundo plano, el servicio de máquina virtual del clúster supervisor aprovisiona el nuevo nodo de trabajo.

8 Compruebe que se agreguen los nodos nuevos.

```
kubectl get tanzukubernetescluster tkgs-cluster-1
```

El plano de control que se amplió horizontalmente ahora tiene 3 nodos.

```
NAME              CONTROL PLANE   WORKER   DISTRIBUTION                       AGE   PHASE
tkgs-cluster-1    3               3        v1.18.5+vmware.1-tkg.1.886c781    1d    running
```

Escalar horizontalmente los nodos de trabajo

Para escalar horizontalmente un clúster de Tanzu Kubernetes, aumente el número de nodos de trabajo mediante kubectl.

1 Realice la autenticación con clúster supervisor.

```
kubectl vsphere login --server=SVC-IP-ADDRESS --vsphere-username USERNAME
```

2 Cambie el contexto al espacio de nombres de vSphere en el que se aprovisiona el clúster de Tanzu Kubernetes.

```
kubectl config use-context tkgs-cluster-ns
```

3 Enumere los clústeres de Kubernetes que se están ejecutando en el espacio de nombres.

```
kubectl get tanzukubernetescluster -n tkgs-cluster-ns
```

4 Obtenga la cantidad de nodos que se ejecutan en el clúster de destino.

```
kubectl get tanzukubernetescluster tkgs-cluster-1
```

Por ejemplo, el siguiente clúster tiene 3 nodo de plano de control y 3 nodos de trabajo.

```
NAME              CONTROL PLANE   WORKER   DISTRIBUTION                       AGE   PHASE
tkgs-cluster-1    3               3        v1.18.5+vmware.1-tkg.1.886c781    1d    running
```

5 Cargue el manifiesto del clúster para editarlo ejecutando el comando `kubectl edit`.

```
kubectl edit tanzukubernetescluster/tkgs-cluster-1
```

El manifiesto del clúster se abrirá en el editor de texto que definan las variables de entorno KUBE_EDITOR o EDITOR.

6 Busque el parámetro `spec.topology.workers.count` y aumente el número de nodos.

```
...
workers:
    count: 3
...
```

```
...
workers:
    count: 4
...
```

7 Para aplicar los cambios, guarde el archivo en el editor de texto. Para cancelar, cierre el editor sin guardar.

Cuando guarde el archivo, kubectl aplicará los cambios al clúster. En segundo plano, el servicio de máquina virtual del clúster supervisor aprovisiona el nuevo nodo de trabajo.

8 Compruebe que se haya agregado el nuevo nodo de trabajo.

```
kubectl get tanzukubernetescluster tkgs-cluster-1
```

Después de ampliar, el clúster tiene 4 nodos de trabajo.

```
NAME              CONTROL PLANE   WORKER   DISTRIBUTION                     AGE   PHASE
tkgs-cluster-1    3               4        v1.18.5+vmware.1-tkg.1.886c781   1d    running
```

Reducir los nodos de trabajo

Para reducir un clúster de Tanzu Kubernetes, reduzca el número de nodos de trabajo. No se admite la reducción en el plano de control.

1 Realice la autenticación con clúster supervisor.

```
kubectl vsphere login --server=SVC-IP-ADDRESS --vsphere-username USERNAME
```

2 Cambie el contexto al espacio de nombres de vSphere en el que se aprovisiona el clúster de Tanzu Kubernetes.

```
kubectl config use-context tkgs-cluster-ns
```

3 Enumere los clústeres de Kubernetes que se están ejecutando en el espacio de nombres.

```
kubectl get tanzukubernetescluster -n tkgs-cluster-ns
```

4 Obtenga la cantidad de nodos que se ejecutan en el clúster de destino.

```
kubectl get tanzukubernetescluster tkgs-cluster-1
```

Por ejemplo, el siguiente clúster tiene 3 nodo de plano de control y 3 nodos de trabajo.

```
NAME               CONTROL PLANE   WORKER   DISTRIBUTION                      AGE   PHASE
tkgs-cluster-1     3               4        v1.18.5+vmware.1-tkg.1.886c781    1d    running
```

5 Cargue el manifiesto del clúster para editarlo ejecutando el comando `kubectl edit`.

```
kubectl edit tanzukubernetescluster/tkgs-cluster-1
```

El manifiesto del clúster se abrirá en el editor de texto que definan las variables de entorno KUBE_EDITOR o EDITOR.

6 Busque el parámetro `spec.topology.workers.count` y aumente el número de nodos.

```
...
workers:
    count: 4
...
```

```
...
workers:
    count: 2
...
```

7 Para aplicar los cambios, guarde el archivo en el editor de texto. Para cancelar, cierre el editor sin guardar.

Cuando guarde el archivo, kubectl aplicará los cambios al clúster. En segundo plano, el servicio de máquina virtual del clúster supervisor aprovisiona el nuevo nodo de trabajo.

8 Compruebe que se hayan agregado los nodos de trabajo.

```
kubectl get tanzukubernetescluster tkgs-cluster-1
```

Después de reducir, el clúster tiene 2 nodos de trabajo.

```
NAME               CONTROL PLANE   WORKER   DISTRIBUTION                      AGE   PHASE
tkgs-cluster-1     3               2        v1.18.5+vmware.1-tkg.1.886c781    1d    running
```

Ampliar un clúster verticalmente

Puede ampliar verticalmente un clúster de Tanzu Kubernetes si cambia la clase de máquina virtual que se utiliza para alojar los nodos del clúster. El ajuste de ampliación vertical es compatible con los nodos de plano de control y de trabajo.

servicio Tanzu Kubernetes Grid admite el escalado vertical de nodos del clúster a través del mecanismo de actualización gradual que está integrado en el servicio. Si cambia la definición de `VirtualMachineClass`, el servicio implementa gradualmente los nodos nuevos con esa nueva clase y reduce la velocidad de los nodos antiguos. Consulte Actualizar clústeres de Tanzu Kubernetes.

1 Realice la autenticación con clúster supervisor.

```
kubectl vsphere login --server=SVC-IP-ADDRESS --vsphere-username USERNAME
```

2 Cambie el contexto al espacio de nombres de vSphere en el que se aprovisiona el clúster de Tanzu Kubernetes.

```
kubectl config use-context tkgs-cluster-ns
```

3 Enumere los clústeres de Kubernetes que se están ejecutando en el espacio de nombres.

```
kubectl get tanzukubernetescluster -n tkgs-cluster-ns
```

4 Describa el clúster de Tanzu Kubernetes de destino y compruebe la clase de máquina virtual.

```
kubectl describe tanzukubernetescluster tkgs-cluster-2
```

Por ejemplo, el siguiente clúster utiliza la clase de máquina virtual best-effort-small.

```

Spec:
  ...
  Topology:
    Control Plane:
      Class:          best-effort-small
      ...
    Workers:
      Class:          best-effort-small
      ...
```

5 Enumere y describa las clases de máquinas virtuales disponibles.

```
kubectl get virtualmachineclassbinding
```

```
kubectl describe virtualmachineclassbinding
```

Nota La clase de máquina virtual que desea utilizar debe estar enlazada al espacio de nombres de vSphere. Consulte Clases de máquina virtual para clústeres de Tanzu Kubernetes.

6 Abra para editar el manifiesto del clúster de destino.

```
kubectl edit tanzukubernetescluster/tkgs-cluster-2
```

El manifiesto del clúster se abrirá en el editor de texto que definan las variables de entorno KUBE_EDITOR o EDITOR.

7 Edite el manifiesto cambiando la clase de máquina virtual.

Por ejemplo, edite el manifiesto del clúster para usar la clase de máquina virtual `guaranteed-xlarge` para el plano de control y los nodos de trabajo.

```
spec:
  topology:
    controlPlane:
      class: guaranteed-xlarge
      ...
    workers:
      class: guaranteed-xlarge
      ...
```

8 Para aplicar los cambios, guarde el archivo en el editor de texto. Para cancelar, cierre el editor sin guardar.

Cuando guarde el archivo, kubectl aplicará los cambios al clúster. En segundo plano, servicio Tanzu Kubernetes Grid aprovisiona los nuevos nodos y elimina los anteriores. Si desea ver una descripción del proceso de actualización gradual, consulte Acerca de las actualizaciones de clústeres de servicio Tanzu Kubernetes Grid.

9 Compruebe que el clúster se esté actualizando.

```
kubectl get tanzukubernetescluster
NAME             CONTROL PLANE   WORKER   DISTRIBUTION                       AGE   PHASE
tkgs-cluster-1   3               3        v1.18.5+vmware.1-tkg.1.c40d30d     21h   updating
```

Eliminar un clúster de Tanzu Kubernetes

Utilice `kubectl` para eliminar un clúster de Tanzu Kubernetes aprovisionado por el servicio Tanzu Kubernetes Grid.

Cuando se elimina un clúster de Tanzu Kubernetes mediante `kubectl`, la recopilación de elementos no utilizados de Kubernetes garantiza que se eliminen todos los recursos dependientes.

Nota No intente eliminar un clúster de Tanzu Kubernetes mediante vSphere Client o la CLI de vCenter Server.

Procedimiento

1 Realice la autenticación con clúster supervisor.

Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

2 Cambie el contexto al espacio de nombres de vSphere donde se aprovisiona la instancia de Tanzu Kubernetes que desea eliminar.

```
kubectl config use-context CLUSTER-NAMESPACE
```

Por ejemplo:

```
kubectl config use-context tkgs-ns-1
```

3 Enumere los clústeres de Tanzu Kubernetes del espacio de nombres.

```
kubectl get clusters
```

Por ejemplo:

```
kubectl get clusters
NAME             PHASE
tkgs-cluster-1   provisioned
```

4 Elimine el clúster de Tanzu Kubernetes mediante la siguiente sintaxis.

```
kubectl delete tanzukubernetescluster --namespace CLUSTER-NAMESPACE CLUSTER-NAME
```

Por ejemplo:

```
kubectl delete tanzukubernetescluster --namespace tkgs-ns-1 tkgs-cluster-1
```

Resultado esperado:

```
tanzukubernetescluster.run.tanzu.vmware.com "tkgs-cluster-1" deleted
```

5 Compruebe que el clúster se haya eliminado.

```
kubectl get clusters
```

Por ejemplo:

```
kubectl get clusters
No resources found in tkgs-ns-1 namespace.
```

6 Elimine el contexto del clúster del archivo `kubeconfig`.

```
kubectl config delete-context CONTEXT
```

Por ejemplo:

```
kubectl config get-contexts
CURRENT   NAME              CLUSTER         AUTHINFO
NAMESPACE
```

```
          192.0.2.1         192.0.2.1        wcp:192.0.2.1:administrator@vsphere.local
          tkgs-cluster-1    192.0.2.6        wcp:192.0.2.6:administrator@vsphere.local
*         tkgs-ns-1         192.0.2.7        wcp:192.0.2.7:administrator@vsphere.local
tkgs-ns-1
```

```
kubectl config delete-context tkgs-cluster-1
deleted context tkgs-cluster-1 from $HOME/.kube/config
```

```
kubectl config get-contexts
CURRENT   NAME              CLUSTER          AUTHINFO
NAMESPACE
          192.0.2.1         192.0.2.1        wcp:192.0.2.1:administrator@vsphere.local
*         tkgs-ns-1         192.0.2.7        wcp:192.0.2.7:administrator@vsphere.local
tkgs-ns-1
```

Especificar un editor de texto predeterminado para Kubectl

Para ayudar a aprovisionar, operar y mantener los clústeres de Tanzu Kubernetes, especifique un editor de texto predeterminado para kubectl.

Propósito

Después de aprovisionar un clúster de Tanzu Kubernetes, debe mantenerlo. Entre las tareas de mantenimiento típicas se incluye la actualización de la versión de Kubernetes y el escalado de los nodos del clúster. Para realizar estas tareas, actualice el manifiesto del clúster.

La manera más cómoda de actualizar el manifiesto de un clúster aprovisionado es utilizar el comando kubectl edit. Este comando abre el manifiesto de Kubernetes en el editor de texto que usted elija. Al guardar los cambios, Kubernetes los aplica automáticamente y actualiza el clúster.

Para utilizar el comando `kubectl edit`, cree una variable de entorno KUBE_EDITOR y especifique el editor de texto preferido como el valor de la variable. Además, anexe la marca de inspección (`-w`) al valor para que kubectl sepa cuándo se confirmaron (se guardaron) los cambios.

Windows

En Windows, cree una variable de entorno del sistema llamada `KUBE_EDITOR` con el valor establecido en la ruta de acceso del editor de texto elegido. Anexe la marca de inspección (`-w`) al valor.

Por ejemplo, la siguiente variable de entorno establece el código de Visual Studio como el editor de texto predeterminado para kubectl e incluye la marca de inspección para que Kubernetes sepa cuándo se guardaron los cambios:

```
KUBE_EDITOR=code -w
```

Mac OS

En Mac OS, cree una variable de entorno llamada `KUBE_EDITOR` con el valor establecido en la ruta de acceso del editor de texto elegido. Anexe la marca de inspección (`-w`) al valor para que kubectl sepa cuándo se confirmaron (se guardaron) los cambios.

Por ejemplo, la siguiente adición a `.bash_profile` establece Sublime como el editor de texto predeterminado para kubectl e incluye la marca de inspección para que kubectl sepa cuándo se guardaron los cambios.

```
export KUBE_EDITOR="/Applications/Sublime.app/Contents/SharedSupport/bin/subl -w"
```

Linux

En Linux (Ubuntu, por ejemplo), la línea de comandos predeterminada `EDITOR` suele ser VIM. Si es así, no se necesita ninguna otra acción para usar el comando `kubectl edit`. Si desea utilizar otro editor, cree una variable de entorno llamada `KUBE_EDITOR` con el valor establecido en la ruta de acceso del editor de texto elegido.

Operar clústeres de Tanzu Kubernetes

servicio Tanzu Kubernetes Grid incluye recursos personalizados que se utilizan para operar clústeres de Tanzu Kubernetes. Además, debido a la estrecha integración con la infraestructura de vSphere, puede utilizar herramientas de vSphere conocidas a modo de ayuda para administrar y mantener clústeres de Tanzu Kubernetes.

Supervisar el estado del clúster de Tanzu Kubernetes mediante kubectl

Puede supervisar el estado de los clústeres de Tanzu Kubernetes aprovisionados mediante kubectl.

Procedimiento

1 Realice la autenticación con clúster supervisor. Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

2 Cambie al espacio de nombres de vSphere en el que se ejecuta el clúster.

```
kubectl config use-context SUPERVISOR-NAMESPACE
```

3 Vea una lista de los clústeres de Tanzu Kubernetes que se ejecutan en el espacio de nombres.

```
kubectl get tanzukubernetesclusters
```

Este comando devuelve el estado del clúster. Si desea ver una descripción de los campos del estado, consulte Estado del ciclo de vida de los clústeres de Tanzu Kubernetes en kubectl.

4 Vea los detalles del clúster.

```
kubectl describe tanzukubernetescluster <cluster-name>
```

El comando devuelve los detalles del clúster. En la sección Estado del resultado del comando, se muestra información detallada del clúster.

```
...
Status:
  Addons:
    Cni:
      Name:    calico
      Status:  applied
    Csi:
      Name:    pvcsi
      Status:  applied
    Psp:
      Name:    defaultpsp
      Status:  applied
  Cloudprovider:
    Name:  vmware-guest-cluster
  Cluster API Status:
    API Endpoints:
      Host:  10.161.90.22
      Port:  6443
    Phase:   provisioned
  Node Status:
    test-tanzu-cluster-control-plane-0:                  ready
    test-tanzu-cluster-workers-0-749458f97c-97ljv:       ready
  Phase:                                                 running
  Vm Status:
    test-tanzu-cluster-control-plane-0:                  ready
    test-tanzu-cluster-workers-0-749458f97c-97ljv:       ready
Events:                                                  <none>
```

5 Ejecute otros comandos `kubectl` para ver más detalles del clúster. Consulte Utilizar comandos operativos del clúster de Tanzu Kubernetes.

Comprobar la preparación del clúster de Tanzu Kubernetes

Cuando el servicio Tanzu Kubernetes Grid aprovisiona un clúster de Tanzu Kubernetes, se notifican varias condiciones de estado que pueden servir para obtener información directa sobre los aspectos clave del estado de la máquina.

Comprobar la preparación de TanzuKubernetesCluster

Puede utilizar las condiciones de preparación de TanzuKubernetesCluster para determinar qué fase o componente no está listo, si es que hay alguno. Consulte Condición y motivos de ControlPlaneReady.

Cuando haya comprobado la preparación del clúster, y para diagnosticar más detalles, puede utilizar capwcluster y las condiciones de máquina para ver más detalles del error. Consulte Comprobar el estado de la máquina de Tanzu Kubernetes y Comprobar el estado del clúster de Tanzu Kubernetes.

Para comprobar la preparación de un clúster de Tanzu Kubernetes:

1 Inicie sesión en clúster supervisor.

2 Cambie el contexto al espacio de nombres donde se aprovisiona el clúster de destino. Por ejemplo:

```
kubectl config use-context tkgs-cluster-ns
```

3 Ejecute el comando `kubectl get tkc -o yaml`. El sistema muestra las condiciones de preparación del clúster. Por ejemplo:

```
status:
  addons:
    authsvc:
      conditions:
      - lastTransitionTime: "2021-01-30T19:53:54Z"
        status: "True"
        type: AuthServiceProvisioned
      name: authsvc
      status: applied
      version: 0.1-66-g8b8f07f
    cloudprovider:
      conditions:
      - lastTransitionTime: "2021-01-30T19:53:53Z"
        status: "True"
        type: CPIProvisioned
      name: vmware-guest-cluster
      status: applied
      version: 0.1-77-g5875817
    cni:
      conditions:
      - lastTransitionTime: "2021-01-30T19:53:53Z"
        status: "True"
        type: CNIProvisioned
      name: calico
      status: applied
      version: 1.16.14+vmware.1-tkg.1.ada4837
    csi:
      conditions:
      - lastTransitionTime: "2021-01-30T19:53:54Z"
        status: "True"
        type: CSIProvisioned
      name: pvcsi
      status: applied
      version: v0.0.1.alpha+vmware.79-7ecdcb1
    dns:
      conditions:
```

```
      - lastTransitionTime: "2021-01-30T19:53:48Z"
        status: "True"
        type: CoreDNSProvisioned
      name: CoreDNS
      status: applied
      version: v1.6.2_vmware.10
    proxy:
      conditions:
      - lastTransitionTime: "2021-01-30T19:53:48Z"
        status: "True"
        type: KubeProxyProvisioned
      name: kube-proxy
      status: applied
      version: 1.16.14+vmware.1
    psp:
      conditions:
      - lastTransitionTime: "2021-01-30T19:53:47Z"
        status: "True"
        type: PSPProvisioned
      name: defaultpsp
      status: applied
      version: v1.16.14+vmware.1-tkg.1.ada4837
  clusterApiStatus:
    apiEndpoints:
    - host: 192.168.1.2
      port: 6443
    phase: Provisioned
  conditions:
  - lastTransitionTime: "2021-01-30T19:53:54Z"
    status: "True"
    type: AddonsReady
  - lastTransitionTime: "2021-01-30T19:51:11Z"
    status: "True"
    type: ControlPlaneReady
  - lastTransitionTime: "2021-01-30T19:51:04Z"
    message: 3/3 Control Plane Node(s) healthy. 1/1 Worker Node(s) healthy
    status: "True"
    type: NodesHealthy
  - lastTransitionTime: "2021-01-31T21:22:45Z"
    status: "True"
    type: ProviderServiceAccountsReady
  - lastTransitionTime: "2021-01-30T19:53:50Z"
    status: "True"
    type: RoleBindingSynced
  - lastTransitionTime: "2021-01-30T19:53:58Z"
    status: "True"
    type: ServiceDiscoveryReady
  - lastTransitionTime: "2021-01-30T19:53:59Z"
    status: "True"
    type: StorageClassSynced
  - lastTransitionTime: "2021-01-27T11:34:53Z"
    status: "True"
    type: TanzuKubernetesReleaseCompatible
  - lastTransitionTime: "2021-01-27T11:34:54Z"
```

```
      message: '[1.17.13+vmware.1-tkg.2.2c133ed]'
      severity: Info
      status: "True"
      type: UpdatesAvailable
```

Condición y motivos de ControlPlaneReady

La tabla enumera y describe la condición `ControlPlaneReady`.

Tabla 13-7. Condición ControlPlaneReady

Tipo de condición	Descripción
`ControlPlaneReady`	Informa sobre si los nodos del plano de control están listos y en funcionamiento para el clúster.

La tabla enumera y describe los motivos por los que la condición `ControlPlaneReady` puede ser falsa.

Tabla 13-8. Motivos falsos de ControlPlaneReady

Motivo	Gravedad	Descripción
`WaitingForClusterInfrastructure`		Indica que el clúster está esperando los requisitos previos necesarios para ejecutar máquinas, como un equilibrador de carga. Este motivo solo se utiliza si InfrastructureCluster no informa de su propia condición de preparación.
`WaitingForControlPlaneInitialized`		Indica que se está inicializando el primer nodo de plano de control.
`WaitingForControlPlane`		Refleja la condición de KubeadmControlPlane. Este motivo se utiliza si KubeadmControlPlane no informa de su propia condición de preparación.
Esperando a que la infraestructura del clúster esté preparada	Mensaje	Indica que el clúster está esperando los requisitos previos necesarios para ejecutar máquinas, como redes y equilibradores de carga.

Condición y motivos de NodesHealthy

La tabla enumera y describe la condición `NodesHealthy`.

Tabla 13-9. Condición de NodesHealthy

Tipo de condición	Descripción
`NodesHealthy`	Informa del estado de los nodos de TanzuKubernetesCluster.

La tabla enumera y describe el motivo por el que la condición `NodesHealthy` no es verdadera.

Tabla 13-10. Motivo falso de NodesHealthy

Motivo	Gravedad	Descripción
WaitingForNodesHealthy		Documenta que no todos los nodos están en buen estado.

Condiciones y motivos de los complementos

En la tabla se enumeran y se describen las condiciones relacionadas con los componentes de complemento del clúster.

Tabla 13-11. Condiciones de los complementos

Tipo de condición	Descripción
AddonsReady	Resumen de condiciones de los complementos de TanzuKubernetesCluster (CoreDNS, KubeProxy, CSP, CPI, CNI, AuthSvc) .
CNIProvisioned	Documenta el estado del complemento de la interfaz de red de contenedor (CNI) de TanzuKubernetesCluster .
CSIProvisioned	Documenta el estado del complemento de la interfaz de almacenamiento de contenedor (CSI) de TanzuKubernetesCluster.
CPIProvisioned	Documenta el estado del complemento de proveedor de nube (CPI) de TanzuKubernetesCluster.
KubeProxyProvisioned	Documenta el estado del complemento KubeProxy de TanzuKubernetesCluster.
CoreDNSProvisioned	Documenta el estado del complemento CoreDNS de TanzuKubernetesCluster.
AuthServiceProvisioned	Documenta el estado del complemento AuthService de TanzuKubernetesCluster.
PSPProvisioned	Documenta el estado de PodSecurityPolicy.

La tabla enumera y describe los motivos por los que las condiciones del complemento no son verdaderas.

Tabla 13-12. Motivos falsos de complementos

Motivo	Gravedad	Descripción
AddonsReconciliationFailed		Motivo resumido de todos los errores de reconciliación de los complementos.
CNIProvisioningFailed	Advertencia	No se pudo crear ni actualizar el complemento CNI de los documentos.
CSIProvisioningFailed	Advertencia	No se pudo crear ni actualizar el complemento CSI de los documentos.

Tabla 13-12. Motivos falsos de complementos (continuación)

Motivo	Gravedad	Descripción
`CPIProvisioningFailed`	Advertencia	No se pudo crear ni actualizar el complemento CPI de los documentos.
`KubeProxyProvisioningFailed`	Advertencia	No se pudo crear ni actualizar el complemento KubeProxy de los documentos.
`CoreDNSProvisioningFailed`	Advertencia	No se pudo crear ni actualizar el complemento de CoreDNS de los documentos.
`AuthServiceProvisioningFailed`	Advertencia	No se pudo crear ni actualizar el complemento de AuthService de los documentos.
`AuthServiceUnManaged`		El controlador no administra AuthService de los documentos.
`PSPProvisioningFailed`	Advertencia	No se pudieron crear ni actualizar los complementos de PodSecurityPolicy de los documentos.

Otras condiciones y motivos

En la tabla se enumeran y describen las condiciones para la sincronización de StorageClass y RoleBinding, la reconciliación de recursos de ProviderServiceAccount, la detección de servicios y la compatibilidad con TanzuKubernetesCluster.

Tabla 13-13. Otras condiciones

Condición	Descripción
`StorageClassSynced`	Documenta el estado de sincronización de StorageClass del clúster supervisor al clúster de carga de trabajo.
`RoleBindingSynced`	Documenta el estado de sincronización de RoleBinding del clúster supervisor al clúster de carga de trabajo.
`ProviderServiceAccountsReady`	Documenta el estado de las cuentas de servicio del proveedor y se crean los Roles, RoleBindings y Secrets relacionados.
`ServiceDiscoveryReady`	Documenta el estado de los descubrimientos del servicio.
`TanzuKubernetesReleaseCompatible`	Indica si TanzuKubernetesCluster es compatible con TanzuKubernetesRelease.

La tabla enumera y describe los motivos por los que otras condiciones no son verdaderas.

Tabla 13-14. Otros motivos

Motivo	Gravedad	Descripción
StorageClassSyncFailed		Informa que la sincronización de StorageClass ha fallado.
RoleBindingSyncFailed		Informa que la sincronización de RoleBinding ha fallado.
ProviderServiceAccountsReconciliationFailed		Informa que la reconciliación de recursos relacionados con las cuentas de servicio del proveedor ha fallado.
SupervisorHeadlessServiceSetupFailed		Documenta que la configuración del servicio sin cabecera para el servidor API del clúster supervisor ha fallado.

Ver la jerarquía de recursos completa de un clúster de Tanzu Kubernetes

Puede ver la jerarquía de recursos completa de un clúster de Tanzu Kubernetes mediante kubectl. Al ver la lista completa de recursos del clúster, podrá determinar los recursos que pueden estar causando problemas.

Requisitos previos

Conéctese al clúster supervisor. Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

Procedimiento

1 Cambie el contexto para utilizar el contexto del clúster de destino.

```
kubectl config use-context CLUSTER-NAME
```

2 Ejecute el siguiente comando para ver el recurso de clúster de la API del clúster.

```
kubectl describe clusters.cluster.x-k8s.io CLUSTER-NAME
```

Este comando devuelve la jerarquía de recursos del clúster designado de la siguiente forma: espacio de nombres, versión de la API, versión del recurso.

Ver el estado del ciclo de vida de los clústeres de Tanzu Kubernetes

El estado del ciclo de vida de los clústeres de Tanzu Kubernetes se puede ver en el inventario de vSphere y con kubectl.

Estado del ciclo de vida de los clústeres de Tanzu Kubernetes en vSphere

En la tabla se incluye y se describe la información del estado de los clústeres de Tanzu Kubernetes que aparece en el inventario de vSphere. Para ver esta información, consulte Supervisar el estado del clúster de Tanzu Kubernetes mediante vSphere Client.

Tabla 13-15. Estado de los clústeres de Tanzu Kubernetes en el inventario de vSphere

Campo	Descripción	Ejemplo
Nombre	Nombre del clúster que define el usuario.	`tkg-cluster-01`
Hora de creación	Fecha y hora de creación del clúster.	`Mar 17, 2020, 11:42:46 PM`
Fase	Estado del ciclo de vida del clúster. Consulte Tabla 13-17. Estado de la fase del ciclo de vida de los clústeres.	`creating`
Número de trabajos	Cantidad de nodos de trabajo del clúster.	`1` o `2` o `5`
Versión de distribución	Versión del software de Kubernetes que se ejecuta en el clúster.	`v1.16.6+vmware.1-tkg.1.7144628`
Dirección del plano de control	Dirección IP del equilibrador de carga del plano de control del clúster.	`192.168.123.2`

Estado del ciclo de vida de los clústeres de Tanzu Kubernetes en kubectl

En la tabla se incluye y se describe la información del estado de los clústeres de Tanzu Kubernetes que aparece en kubectl. Para ver esta información, consulte Supervisar el estado del clúster de Tanzu Kubernetes mediante kubectl.

Tabla 13-16. Estado de los clústeres de Tanzu Kubernetes en kubectl

Campo	Descripción	Ejemplo
NAME	Nombre del clúster.	`tkg-cluster-01`
CONTROL PLANE	Cantidad de nodos del plano de control del clúster.	`3`
WORKER	Cantidad de nodos de trabajo del clúster.	`5`
DISTRIBUTION	Versión de Kubernetes que ejecuta el clúster.	`v1.16.6+vmware.1-tkg.1.5b5608b`
AGE	Cantidad de días de ejecución del clúster.	`13d`
PHASE	Estado del ciclo de vida del clúster. Consulte Tabla 13-17. Estado de la fase del ciclo de vida de los clústeres.	`running`

Estado de la fase del ciclo de vida de los clústeres

En la tabla se enumera y se describe el estado de cada fase del ciclo de vida de los clústeres. Consulte Tabla 13-17. Estado de la fase del ciclo de vida de los clústeres.

Tabla 13-17. Estado de la fase del ciclo de vida de los clústeres

Fase	Descripción
`creating`	El aprovisionamiento de clústeres puede comenzar, el plano de control se está creando o el plano de control se crea pero no se inicializa.
`deleting`	El clúster se está eliminando.
`failed`	Se produjo un error en la creación del plano de control del clúster y es probable que el usuario tenga que intervenir de alguna forma.
`running`	La infraestructura se crea y se configura, y el plano de control se inicializa por completo.
`updating`	El clúster se está actualizando.

Utilizar comandos operativos del clúster de Tanzu Kubernetes

Puede administrar clústeres de Tanzu Kubernetes mediante los comandos kubectl personalizados. Estos comandos se ponen a disposición de los recursos personalizados creados por el servicio Tanzu Kubernetes Grid.

Comandos personalizados para administrar clústeres de Tanzu Kubernetes

En la tabla se enumeran y describen comandos kubectl para administrar clústeres de Tanzu Kubernetes.

Tabla 13-18. Comandos personalizados para administrar clústeres de Tanzu Kubernetes

Comando	Descripción
`kubectl get tanzukubernetescluster`	Enumera los clústeres del espacio de nombres actual.
`kubectl get tkc`	Versión de formato corto del comando anterior.
`kubectl describe tanzukubernetescluster CLUSTER-NAME`	Describe el clúster especificado mostrando el estado, la condición y los eventos expresados. Cuando se completa el aprovisionamiento, este comando muestra la IP virtual creada para el equilibrador de carga que presenta los endpoints de la API de Kubernetes.
`kubectl get cluster-api`	Enumera los recursos de la API del clúster que respaldan los clústeres en el espacio de nombres actual, incluidos los recursos del proyecto de la API del clúster y del proveedor de la API del clúster que el servicio Tanzu Kubernetes Grid utiliza.
`kubectl get tanzukubernetesreleases`	Lista de las versiones de Tanzu Kubernetes disponibles.
`kubectl get tkr`	Versión de formato corto del comando anterior.
`kubectl get tkr v1.17.8---vmware.1-tkg.1.5417466 -o yaml`	Proporciona detalles sobre la versión de Tanzu Kubernetes con nombre.

Tabla 13-18. Comandos personalizados para administrar clústeres de Tanzu Kubernetes (continuación)

Comando	Descripción
`kubectl get virtualmachine`	Enumera los recursos de la máquina virtual que respaldan los nodos del clúster en el espacio de nombres actual.
`kubectl get vm`	Versión de formato corto del comando anterior.
`kubectl describe virtualmachine VIRTUAL-MACHINE-NAME`	Describe la máquina virtual especificada a través del estado actual y los eventos.
`kubectl describe virtualmachinesetresourcepolicy`	Enumera los recursos de directiva de recursos establecidos en la máquina virtual que respaldan el clúster en el espacio de nombres actual. Este recurso representa el grupo de recursos y la carpeta de objetos de vSphere que se usan para el clúster.
`kubectl get virtualmachineservice`	Enumera los recursos de servicio de la máquina virtual que respaldan los nodos del clúster en el espacio de nombres actual. Estos recursos son análogos a un servicio, pero para máquinas virtuales en lugar de pods. Los servicios de la máquina virtual se utilizan para proporcionar un equilibrador de carga para los nodos del plano de control de un clúster y para el proveedor de nube paravirtual con el fin de admitir un servicio de Kubernetes de tipo LoadBalancer dentro de un clúster. Consulte también el comando `kubectl loadbalancer`.
`kubectl get vmservice`	Versión de formato corto del comando anterior.
`kubectl describe virtualmachineservice` *`VIRTUAL-MACHINE-SERVICE-NAME`*	Describe el servicio de la máquina virtual especificada a través del estado deseado del clúster, el estado actual y los eventos.
`kubectl get virtualmachineimage`	Lista de las versiones de Tanzu Kubernetes disponibles.
`kubectl get vmimage`	Versión de acceso directo del comando anterior.
`kubectl describe vmimage VM_IMAGE_NAME`	Vea los detalles de la imagen de la máquina virtual con nombre.
`kubectl get loadbalancer`	Enumera los recursos del equilibrador de carga en el espacio de nombres actual, incluidos los que se utilizan para clústeres. Se crea un equilibrador de carga para el servicio de la máquina virtual.
`kubectl get virtualnetwork`	Enumera los recursos de la red virtual en el espacio de nombres actual, incluidos los recursos que se utilizan para clústeres. Se crea una red virtual para cada espacio de nombres en el que se aprovisiona un clúster, así como para cada clúster en sí.

Tabla 13-18. Comandos personalizados para administrar clústeres de Tanzu Kubernetes (continuación)

Comando	Descripción
`kubectl get persistentvolumeclaim`	Enumera los recursos de notificación de volumen persistente en el espacio de nombres actual, incluidos los que se utilizan para clústeres. Consulte Capítulo 10 Usar almacenamiento persistente en vSphere with Tanzu.
`kubectl get cnsnodevmattachment`	Enumera los recursos de asociación de máquinas virtuales del nodo de CNS en el espacio de nombres actual. Estos recursos representan la asociación de un volumen persistente administrado por CNS con una máquina virtual que actúa como el nodo de un clúster. Consulte Capítulo 10 Usar almacenamiento persistente en vSphere with Tanzu.
`kubectl get configmap`	Enumera los mapas de configuración en el espacio de nombres actual, incluidos los que se utilizan para crear nodos del clúster. Los mapas de configuración no están pensados para que el usuario pueda modificarlos, y cualquier cambio realizado se sobrescribirá.
`kubectl get secret`	Enumera los secretos del espacio de nombres actual, incluidos los que se utilizan para crear y administrar nodos del clúster. Consulte Obtener los secretos del clúster de Tanzu Kubernetes.

Utilizar comandos de redes del clúster de Tanzu Kubernetes

El servicio Tanzu Kubernetes Grid aprovisiona clústeres de Tanzu Kubernetes con redes predeterminadas para los nodos, los pods y los servicios. Puede comprobar las redes del clúster mediante los comandos kubectl personalizados.

Comandos personalizados para comprobar las redes de clústeres de Tanzu Kubernetes

Consulte los siguientes comandos para comprobar las redes del clúster.

Tabla 13-19. Comandos kubectl personalizados para verificar las redes de clústeres

Comando	Descripción
Cambie el contexto al espacio de nombres de vSphere. Por ejemplo: `kubectl config use-context tkgs-ns` Ejecute el comando. `kubectl get tkgserviceconfigurations` Resultado de ejemplo. `NAME                         DEFAULT CNI` `tkg-service-configuration    antrea`	Devuelve la CNI predeterminada, que es `antrea` a menos que se cambie. La CNI predeterminada se utiliza para la creación del clúster, a menos que se anule explícitamente en el YAML del clúster. Para cambiar la CNI predeterminada, consulte Ejemplos de configuración de la API de servicio Tanzu Kubernetes Grid v1alpha1.
Cambie el contexto al espacio de nombres de vSphere. Por ejemplo: `kubectl config use-context tkgs-ns` Ejecute el comando. `kubectl get virtualnetwork` Resultado de ejemplo. `NAME                    SNAT` `READY   AGE` `tkgs-cluster-12-vnet    10.191.152.133` `True    4h3m`	Devuelve la red virtual para los nodos del clúster. Se usa para comprobar que la dirección IP de la traducción de direcciones de red (Network Address Translation, SNAT) de origen esté asignada.

Tabla 13-19. Comandos kubectl personalizados para verificar las redes de clústeres (continuación)

<table>
<tr><th>Comando</th><th>Descripción</th></tr>
<tr><td>Cambie el contexto al espacio de nombres de vSphere. Por ejemplo:
<pre>kubectl config use-context tkgs-ns</pre>Ejecute el comando.
<pre>kubectl get virtualmachines -o wide</pre>Resultado de ejemplo.
<pre>NAME
POWERSTATE   CLASS
IMAGE
PRIMARY-IP   AGE
tkgs-cluster-12-control-plane-...
poweredOn   guaranteed-medium
ob-...-v1.21.6---vmware.1-tkg.1.b3d708a
10.244.0.66   4h6m
tkgs-cluster-12-worker-...
poweredOn   guaranteed-medium
ob-...-v1.21.6---vmware.1-tkg.1.b3d708a
10.244.0.68   4h3m
tkgs-cluster-12-worker-...
poweredOn   guaranteed-medium
ob-...-v1.21.6---vmware.1-tkg.1.b3d708a
10.244.0.67   4h3m</pre></td><td>Devuelve la interfaz de red virtual para los nodos del clúster.
Se usa para comprobar que la máquina virtual de cada nodo del clúster tiene una dirección IP asignada.</td></tr>
<tr><td>Cambie el contexto al espacio de nombres de vSphere. Por ejemplo:
<pre>kubectl config use-context tkgs-ns</pre>Ejecute el comando.
<pre>kubectl get virtualmachineservices</pre>Resultado de ejemplo.
<pre>NAME
TYPE   AGE
tkgs-cluster-12-control-plane-service
LoadBalancer   3h53m</pre></td><td>Devuelve el servicio de la máquina virtual para cada nodo del clúster.
Se usa para comprobar que el estado esté actualizado e incluya la dirección IP virtual (VIP) del equilibrador de carga.</td></tr>
</table>

Tabla 13-19. Comandos kubectl personalizados para verificar las redes de clústeres (continuación)

Comando	Descripción
Cambie el contexto al espacio de nombres del clúster de TKGS. Por ejemplo. `kubectl config use-context tkgs-cluster-10` Ejecute el comando. `kubectl get services -n NAMESPACE` Compruebe lo siguiente. `curl -k https://EXTERNAL-IP:PORT/healthz`	Devuelve el equilibrador de carga del servicio de Kubernetes creado para acceder a la API del clúster. Se usa para comprobar que se asignó una dirección IP externa. Use `curl` para comprobar que se puede acceder a la API mediante la dirección IP externa y el puerto del servicio del equilibrador de carga.
Cambie el contexto al espacio de nombres de vSphere. Por ejemplo: `kubectl config use-context tkgs-ns` Ejecute el comando. `kubectl get endpoints` Resultado de ejemplo. `NAME` `ENDPOINTS           AGE` `tkgs-cluster-12-control-plane-service` `10.244.0.66:6443   3h44m`	Devuelve los nodos del plano de control (endpoints) del clúster. Se usa para comprobar que cada endpoint se cree e incluya en el grupo de endpoints.

Obtener los secretos del clúster de Tanzu Kubernetes

Los clústeres de Tanzu Kubernetes usan secretos para almacenar tokens, claves y contraseñas para los clústeres operativos de Tanzu Kubernetes.

Lista de secretos de los clústeres de Tanzu Kubernetes

Un secreto de Kubernetes es un objeto que almacena una pequeña cantidad de datos confidenciales, como una contraseña, un token o una clave SSH. Es posible que los administradores de clústeres de Tanzu Kubernetes usen varios secretos mientras utilizan los clústeres. En la tabla se enumeran y describen los secretos clave que podrían utilizar los administradores de clústeres.

Nota La lista no es exhaustiva; solo incluye esos secretos que habría que rotar manualmente o que habría que usar para acceder a nodos de clústeres con fines de solución de problemas.

Secreto	Descripción
TANZU-KUBERNETES-CLUSTER-NAME-ccm-token-RANDOM	Un token de cuenta de servicio utilizado por el administrador de controladoras de nube del proveedor de nube paravirtual para conectarse al espacio de nombres de vSphere. Para activar la rotación de esta credencial, elimine el secreto.
TANZU-KUBERNETES-CLUSTER-NAME-pvcsi-token-RANDOM	Un token de cuenta de servicio utilizado por el complemento de CSI paravirtual para conectarse a espacio de nombres de vSphere. Para activar la rotación de esta credencial, elimine el secreto. Consulte Cómo se integra vSphere with Tanzu con el almacenamiento de vSphere.
TANZU-KUBERNETES-CLUSTER-NAME-kubeconfig	Un archivo kubeconfig que se puede utilizar para conectarse al plano de control del clúster como el usuario `kubernetes-admin`. Este secreto se puede utilizar para acceder a un clúster y solucionar los problemas que surjan en él cuando la autenticación de vCenter Single Sign-On no esté disponible. Consulte Conectarse al plano de control del clúster de Tanzu Kubernetes como el administrador.
TANZU-KUBERNETES-CLUSTER-NAME-ssh	Una clave privada SSH que se puede utilizar para conectarse a cualquier nodo del clúster como `vmware-system-user`. Este secreto se puede utilizar para usar SSH en cualquier nodo del clúster y solucionar los problemas. Consulte Conectarse mediante SSH a nodos de clúster de Tanzu Kubernetes como usuario del sistema con una clave privada.
TANZU-KUBERNETES-CLUSTER-NAME-ssh-password	Una contraseña que se puede utilizar para conectarse a cualquier nodo del clúster como `vmware-system-user`. Consulte Conectarse mediante SSH a nodos de clúster de Tanzu Kubernetes como usuario del sistema con una clave privada.
TANZU-KUBERNETES-CLUSTER-NAME-ca	El certificado de CA raíz para el plano de control del clúster de Tanzu Kubernetes que `kubectl` utiliza a fin de conectarse de forma segura al servidor de API de Kubernetes.

Comprobar el estado de la máquina de Tanzu Kubernetes

Cuando el servicio Tanzu Kubernetes Grid aprovisiona un clúster de Tanzu Kubernetes, se notifican varias condiciones de estado que pueden servir para obtener información directa sobre los aspectos clave del estado de la máquina.

Acerca de las condiciones de estado de las máquinas

Un clúster de Tanzu Kubernetes aprovisionado por servicio Tanzu Kubernetes Grid incluye varias partes móviles, todas controladas por controladores independientes pero relacionados que funcionan de forma conjunta para compilar y mantener un conjunto de nodos de Kubernetes. El objeto del `TanzuKubernetesCluster` proporciona condiciones de estado que aportan información detallada sobre el estado de la máquina.

Comprobar el estado de la máquina

Para comprobar el estado de una máquina de Tanzu Kubernetes:

1 Ejecute el comando `kubectl describe machine`.

  Si el estado es Listo, quiere decir que la máquina está en buen estado. Sin embargo, si la condición de una máquina es "false", como `InfrastructureReady`, quiere decir que la máquina no está lista.

2 En ese caso, si la máquina no está lista, ejecute el siguiente comando y determine qué problema hay en la infraestructura:

```
kubectl describe wcpmachine
```

Lista de condiciones de mantenimiento de máquinas

En la tabla se enumeran y se definen las condiciones de estado de las máquinas disponibles para un clúster de Tanzu Kubernetes.

Condición	Descripción
`ResourcePolicyReady`	Notifica la creación de una directiva de recursos.
`ResourcePolicyCreationFailed`	Se indica cuando se producen errores durante la creación de ResourcePolicy.
`ClusterNetworkReady`	Notifica el aprovisionamiento correcto de una red de clústeres.
`ClusterNetworkProvisionStarted`	Se indica mientras se espera a que la red del clúster esté lista.
`ClusterNetworkProvisionFailed`	Se indica cuando se producen errores durante el aprovisionamiento de la red.
`LoadBalancerReady`	Informa sobre la reconciliación correcta de un Endpoint de plano de control estático.
`LoadBalancerCreationFailed`	Se indica cuando se produce un error al crear los recursos relacionados con el equilibrador de carga.
`WaitingForLoadBalancerIP`	Se indica mientras se espera a que haya una dirección IP del equilibrador de carga.
`VMProvisioned`	Informa de que se ha creado una máquina virtual, se ha encendido y se le ha asignado una dirección IP.
`WaitingForBootstrapData`	Se indica cuando una vSphereMachine espera a que el script de arranque esté listo antes de iniciar el proceso de aprovisionamiento.
`VMCreationFailed`	Informa de que ha habido un error en la creación del CRD de la máquina virtual o el correspondiente ConfigMap de arranque.
`VMProvisionStarted`	Se indica cuando una máquina virtual se encuentra en el proceso de creación.

Condición	Descripción
PoweringOn	Se indica cuando una máquina virtual ejecuta en ese momento la secuencia de encendido.
WaitingForNetworkAddress	Se indica cuando se espera a que se active la configuración de red de la máquina.
WaitingForBIOSUUID	Se indica cuando se espera a que la máquina tenga un UUID de BIOS.

Campos de condición

Cada condición puede contener varios campos.

Type	Describe el tipo de condición. Por ejemplo, ResourcePolicyReady. En el caso de la condición Ready, se trata de un resumen de todas las demás condiciones.
Status	Describe el estado del tipo. Los estados pueden ser True, False o Unknown.
Severity	Clasificación de Reason. Info significa que se está realizando la reconciliación. Warning significa que es posible que haya algo mal y vuelva a intentarlo. Error significa que se ha producido un error y hay que llevar a cabo una acción manual para resolverlo.
Reason	Proporciona un motivo por el cual el estado es False. Puede ser que haya que esperar a que esté listo o a que se indique el motivo de un error. Por lo general, se produce cuando el estado es False.
Message	Información de lenguaje natural que explica el significado de Reason.

Comprobar el estado del clúster de Tanzu Kubernetes

Cuando servicio Tanzu Kubernetes Grid aprovisiona un clúster de Tanzu Kubernetes, se notifican varias condiciones de estado que pueden servir para obtener información directa sobre los aspectos clave del estado del clúster.

Acerca de las condiciones de estado del clúster

Un clúster de Tanzu Kubernetes aprovisionado por servicio Tanzu Kubernetes Grid incluye varias partes móviles, todas controladas por controladores independientes pero relacionados que funcionan de forma conjunta para compilar y mantener un conjunto de nodos de Kubernetes. El objeto del TanzuKubernetesCluster proporciona condiciones de estado que aportan información detallada sobre el estado de la máquina y del clúster.

Comprobar estado del clúster

Para comprobar el estado de un clúster de Tanzu Kubernetes:

1 Ejecute el comando `kubectl describe cluster`.

Si el estado es listo, quiere decir que tanto la infraestructura del clúster como el plano de control del clúster están listos. Por ejemplo:

```
Status:
  Conditions:
    Last Transition Time:     2020-11-24T21:37:32Z
    Status:                   True
    Type:                     Ready
    Last Transition Time:     2020-11-24T21:37:32Z
    Status:                   True
    Type:                     ControlPlaneReady
    Last Transition Time:     2020-11-24T21:31:34Z
    Status:                   True
    Type:                     InfrastructureReady
```

Sin embargo, si la condición de un clúster es "false", quiere decir que el clúster no está listo y un campo de mensaje describe lo que está mal. Por ejemplo, a continuación se muestra que el estado es "False" y el motivo por el que la infraestructura no está lista:

```
Status:
  Conditions:
    Last Transition Time:     2020-11-24T21:37:32Z
    Status:                   False
    Type:                     Ready
    Last Transition Time:     2020-11-24T21:37:32Z
    Status:                   True
    Type:                     ControlPlaneReady
    Last Transition Time:     2020-11-24T21:31:34Z
    Status:                   False
    Type:                     InfrastructureReady
```

2 Si el clúster no está listo, ejecute el siguiente comando para determinar qué problema hay en la infraestructura del clúster:

```
kubectl describe wcpcluster
```

Lista de condiciones de estado del clúster

En la tabla se enumeran y se definen las condiciones de estado disponibles para un clúster de Tanzu Kubernetes.

Condición	Descripción
`Ready`	Resume el estado operativo de un objeto de API del clúster.
`Deleting`	El estado no es true porque el objeto subyacente se está eliminando en este momento.
`DeletionFailed`	El estado no es true debido a que el objeto subyacente detectó problemas durante la eliminación. Es una advertencia, porque el reconciliador volverá a intentar la eliminación.

Condición	Descripción
`Deleted`	El estado no es true porque el objeto subyacente se eliminó.
`InfrastructureReady`	Informa de un resumen del estado actual del objeto de infraestructura definido para este clúster.
`WaitingForInfrastructure`	Se indica cuando un clúster espera a que la infraestructura subyacente esté disponible. NOTA: Esta condición se utiliza como reserva cuando la infraestructura no notifica que esté lista.
`ControlPlaneReady`	Se indica cuando el plano de control del clúster está listo.
`WaitingForControlPlane`	Se indica cuando un clúster espera a que el plano de control esté disponible. NOTA: Esta condición se utiliza como reserva cuando el plano de control no notifica que esté listo.

Campos de condición

Cada condición puede contener varios campos.

`Type`	Describe el tipo de condición. Por ejemplo, `ControlPlaneReady`. En el caso de la condición `Ready`, se trata de un resumen de todas las demás condiciones.
`Status`	Describe el estado del tipo. Los estados pueden ser `True`, `False` o `Unknown`.
`Severity`	Clasificación de `Reason`. `Info` significa que se está realizando la reconciliación. `Warning` significa que es posible que haya algo mal y vuelva a intentarlo. `Error` significa que se ha producido un error y hay que llevar a cabo una acción manual para resolverlo.
`Reason`	Proporciona un motivo por el cual el estado es `False`. Puede ser que haya que esperar a que esté listo o a que se indique el motivo de un error. Por lo general, se produce cuando el estado es `False`.
`Message`	Información de lenguaje natural que explica el significado de `Reason`.

Supervisar el estado del clúster de Tanzu Kubernetes mediante vSphere Client

Puede supervisar el estado de los clústeres de Tanzu Kubernetes mediante vSphere Client.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 En el **Menú**, seleccione la vista **Hosts y clústeres**.

3 Expanda los objetos de **Centro de datos > Clúster** en los que se crea clúster supervisor.

4 Expanda el grupo de recursos **Espacios de nombres**.

5 Seleccione el espacio de nombres de vSphere en el que implementó el clúster de Tanzu Kubernetes.

   Cada clúster de Tanzu Kubernetes aparece como una carpeta dentro de su grupo de recursos de espacio de nombres. Cada Tanzu Kubernetes se representa gráficamente con tres iconos de hexágono junto a su nombre.

6 Cambie a la vista **Menú > Máquinas virtuales y plantillas**.

   Dentro de la carpeta del clúster, verá las máquinas virtuales que conforman los nodos del clúster.

7 Seleccione el espacio de nombres de vSphere y, a continuación, seleccione la pestaña **Cálculo**.

8 En **Recursos de VMware**, seleccione **Tanzu Kubernetes**.

   Se mostrará cada clúster de Tanzu Kubernetes que se haya implementado en este espacio de nombres de vSphere. Si desea ver una descripción de cada campo del estado, consulte Estado del ciclo de vida de los clústeres de Tanzu Kubernetes en vSphere.

Implementar cargas de trabajo y paquetes en clústeres TKGS 14

Consulte el contenido de esta sección para instalar cargas de trabajo y paquetes en clústeres de Tanzu Kubernetes.

Este capítulo incluye los siguientes temas:

- Implementar cargas de trabajo en clústeres de Tanzu Kubernetes
- Implementar paquetes TKG en clústeres de Tanzu Kubernetes
- Implementar cargas de trabajo de AI/ML en clústeres de Tanzu Kubernetes

Implementar cargas de trabajo en clústeres de Tanzu Kubernetes

Puede implementar cargas de trabajo de aplicaciones en clústeres de Tanzu Kubernetes mediante pods, servicios, volúmenes persistentes y recursos de nivel superior, como implementaciones y conjuntos de réplicas.

Implementar una carga de trabajo de prueba en un clúster de Tanzu Kubernetes

Después de aprovisionar un clúster de Tanzu Kubernetes, se recomienda implementar una carga de trabajo de prueba y validar la funcionalidad del clúster.

Utilice la aplicación de demostración de kuard para comprobar que el clúster de Tanzu Kubernetes esté activo y en ejecución.

Requisitos previos

- Aprovisionar un clúster de Tanzu Kubernetes. Consulte Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS.
- Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On

Procedimiento

1 Cambie el contexto de configuración al clúster de Tanzu Kubernetes de destino.

```
kubectl config use-context TANZU-KUBERNETES-CLUSTER-NAME
```

Por ejemplo:

```
kubectl config use-context tkgs-cluster-1
Switched to context "tkgs-cluster-1".
```

2 Implemente la aplicación de demostración de `kuard`.

```
kubectl run --restart=Never --image=gcr.io/kuar-demo/kuard-amd64:blue kuard
```

Resultado esperado:

```
pod/kuard created
```

3 Compruebe que el pod se esté ejecutando.

```
kubectl get pods
```

Resultado esperado:

```

NAME                     READY   STATUS    RESTARTS   AGE
kuard                    1/1     Running   0          10d
```

4 Reenvíe el puerto de contenedor 8080 del pod al puerto 8080 de host local.

```
kubectl port-forward kuard 8080:8080
```

Resultado esperado:

```
Forwarding from 127.0.0.1:8080 -> 8080
Forwarding from [::1]:8080 -> 8080
Handling connection for 8080
```

5 En un navegador, vaya a http://localhost:8080.

Aparecerá la página web de la aplicación de demostración de kuard, con la que puede interactuar y verificar aspectos del clúster. Por ejemplo, realice sondeos de estado y de preparación.

6 Para detener el enrutamiento de puerto, presione `Ctrl+C` en la sesión de kubectl.

7 Elimine el pod de `kuard`.

```
kubectl delete pod kuard
```

Resultado esperado:

```
pod "kuard" deleted
```

8 Compruebe que el pod se haya eliminado.

```
kubectl get pods
```

Instalar y ejecutar Octant

Puede instalar la interfaz web de Octant para poder visualizar las cargas de trabajo del clúster de Tanzu Kubernetes, los espacios de nombres y los metadatos, entre otros.

Acerca de Octant

Octant es una interfaz web de código abierto que permite ver los clústeres de Kubernetes y sus aplicaciones.

Instale y ejecute Octant en el mismo cliente en el que ejecuta `kubectl`. A continuación se proporcionan instrucciones de instalación para las plataformas comunes. Para obtener más información, consulte el sitio de Octant.

Una vez que se instala Octant, para utilizarlo, inicie sesión en el clúster de Tanzu Kubernetes con `kubectl` y ejecute el comando `octant`.

Instalar Octant en Windows

Instale el administrador de paquetes de Chocolatey para Windows PowerShell.

Ejecute una sesión de PowerShell como administrador.

Instale Octant mediante el siguiente comando:

```
choco install octant --confirm
```

Instalar Octant en Mac

Instale el administrador de paquetes de Homebrew.

Instale Octant con el siguiente comando:

```
brew install octant
```

Instalar Octant en Ubuntu

Descargue el archivo `.deb` desde la página de versiones.

Instálelo mediante el comando `dpkg -i`.

Ejemplo del servicio del equilibrador de carga de Tanzu Kubernetes

Para aprovisionar un equilibrador de carga externo en un clúster de Tanzu Kubernetes, puede crear un servicio de tipo LoadBalancer. El servicio del equilibrador de carga expone una dirección IP pública. El tráfico desde el equilibrador de carga externo se puede dirigir a los pods del clúster.

Puede aprovisionar un equilibrador de carga externo para los pods de Kubernetes que se exponen como servicios. Por ejemplo, puede implementar un contenedor de Nginx y exponerlo como servicio de Kubernetes de tipo LoadBalancer.

Requisitos previos

- Revise el tipo de servicio LoadBalancer en la documentación de Kubernetes.
- Aprovisionar un clúster de Tanzu Kubernetes. Consulte Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS.
- Conéctese al clúster de Tanzu Kubernetes de destino. Consulte Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.

Procedimiento

1 Cree un enlace de funciones adecuado para la PSP con privilegios predeterminada. Consulte Ejemplo de enlaces de funciones para la directiva de seguridad de pods.

2 Cree el siguiente archivo YAML `nginx-lbsvc.yaml`.

Este archivo YAML define un servicio de Kubernetes de tipo LoadBalancer e implementa un contenedor de Nginx como un equilibrador de carga externo para el servicio.

```
kind: Service
apiVersion: v1
metadata:
  name: srvclb-ngnx
spec:
  selector:
    app: hello
    tier: frontend
  ports:
  - protocol: "TCP"
    port: 80
    targetPort: 80
  type: LoadBalancer
---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: loadbalancer
spec:
  replicas: 2
  selector:
    matchLabels:
      app: hello
  template:
    metadata:
      labels:
        app: hello
        tier: frontend
    spec:
      containers:
      - name: nginx
        image: "nginxdemos/hello"
```

3 Aplique el archivo YAML.

```
kubectl apply -f nginx-lbsvc.yaml
```

4 Compruebe la implementación del servicio nginx.

```
kubectl get services
```

`srvclb-ngnx` tiene una dirección IP externa e interna.

```
NAME          TYPE           CLUSTER-IP      EXTERNAL-IP     PORT(S)         AGE
srvclb-ngnx   LoadBalancer   10.11.12.19     10.19.15.89     80:30818/TCP    18m
```

5 Desde un navegador, introduzca la dirección IP externa del servicio LoadBalancer de Nginx.

Verá un mensaje con el banner de `NGINX` y los detalles del equilibrador de carga.

Equilibrador de carga de servicio de Tanzu Kubernetes con una dirección IP estática (ejemplo)

Puede configurar un servicio de Kubernetes de tipo LoadBalancer para que utilice una dirección IP estática. Tenga en cuenta los requisitos de componente mínimos, un importante aspecto sobre seguridad y las instrucciones de fortalecimiento del clúster cuando implemente esta función.

Requisitos mínimos

Las direcciones IP estáticas para servicios de Kubernetes de tipo equilibrador de carga son compatibles en los clústeres de Tanzu Kubernetes que cumplen con los siguientes requisitos:

Componente	Requisito mínimo	Más información
vCenter Server y ESXi	vSphere 7.0 Update 2	Consulte las notas de la versión.
Clúster supervisor	`v1.19.1+vmware.2-vsc0.0.8-17610687`	Consulte Actualizar clúster supervisor mediante una actualización de los espacios de nombres de vSphere.
Equilibrador de carga	NSX-T Data Center v3.1 O NSX Advanced 20.1.x	Consulte las notas de la versión.
Versión de Tanzu Kubernetes	Una de las versiones más recientes de Tanzu Kubernetes.	Consulte Comprobar la compatibilidad del clúster de Tanzu Kubernetes para actualizar.

Usar una IP estática en un servicio de tipo LoadBalancer

Por lo general, cuando se define un servicio de Kubernetes de Tipo LoadBalancer, el equilibrador de carga asigna una dirección IP efímera. Consulte Ejemplo del servicio del equilibrador de carga de Tanzu Kubernetes.

También puede especificar una dirección IP estática para el equilibrador de carga. Al crear el servicio, la instancia del equilibrador de carga se aprovisiona con la dirección IP estática que asignó.

El siguiente servicio de ejemplo demuestra cómo configurar un equilibrador de carga compatible con una dirección IP estática. En la especificación de servicio, se incluyen el parámetro `loadBalancerIP` y un valor de dirección IP, el cual es `10.11.12.49` en este ejemplo.

```
kind: Service
apiVersion: v1
metadata:
  name: load-balancer-service-with-static-ip
spec:
  selector:
    app: hello-world
    tier: frontend
  ports:
  - protocol: "TCP"
    port: 80
    targetPort: 80
  type: LoadBalancer
  loadBalancerIP: 10.11.12.49
```

Para NSX Advanced Load Balancer, utilice una dirección IP del grupo de IPAM que se configuró para el equilibrador de carga cuando se instaló. Cuando se crea el servicio y se asigna la dirección IP estática, el equilibrador de carga la marca como asignada y administra el ciclo de vida de la dirección IP de la misma forma que una dirección IP efímera. Es decir, si se elimina el servicio, la dirección IP no está asignada y se vuelve disponible para reasignarla.

En el caso del equilibrador de carga de NSX-T, tiene dos opciones. El mecanismo predeterminado es el mismo que en NSX Advanced Load Balancer: utilice una dirección IP tomada del grupo de direcciones IP que se configuró para el equilibrador de carga cuando se instaló. Cuando se asigna la dirección IP estática, el equilibrador de carga la marca automáticamente como asignada y administra su ciclo de vida.

La segunda opción de NSX-T consiste en preasignar manualmente la dirección IP estática. En este caso, se utiliza una dirección IP que no forma parte del grupo de direcciones IP del equilibrador de carga externo asignado al equilibrador de carga, sino que se toma de un grupo de direcciones IP flotantes. En este caso, administra manualmente la asignación y el ciclo de vida de la dirección IP mediante NSX Manager.

Requisitos importantes de fortalecimiento y consideración de seguridad

Puede producirse un problema de seguridad que se debe tener en cuenta al utilizar esta función. Si un desarrollador puede revisar el valor de `Service.status.loadBalancerIP`, es posible que el desarrollador pueda secuestrar el tráfico en el clúster destinado para la dirección IP con revisiones. En concreto, si una función o ClusterRole con el permiso `patch` está enlazada a una cuenta de usuario o servicio en un clúster donde esté implementada esta función, ese propietario de cuenta puede usar sus propias credenciales para emitir comandos `kubectl` y cambiar la dirección IP estática asignada al equilibrador de carga.

Para evitar las posibles implicaciones de seguridad que tiene usar la asignación de direcciones IP estáticas para un servicio de equilibrador de carga, debe fortalecer cada clúster en el que vaya a implementar esta función. Para ello, la función o ClusterRole que defina para cualquier desarrollador no debe permitir el verbo `patch` para `apiGroups:""` y `resources: services/status`. El fragmento de función de ejemplo demuestra lo que no se debe hacer al implementar esta función.

NO PERMITIR LA REVISIÓN

```
- apiGroups:
  - ""
  resources:
  - services/status
  verbs:
  - patch
```

Para comprobar si un desarrollador tiene permisos de revisión, ejecute el siguiente comando como ese usuario:

```
kubectl --kubeconfig <KUBECONFIG> auth can-i patch service/status
```

Si el comando devuelve `yes`, el usuario tiene permisos de revisión. Consulte Comprobación de acceso a la API (Checking API Access) en la documentación de Kubernetes para obtener más información.

Para conceder al desarrollador acceso a un clúster, consulte Conceder acceso de desarrollador a clústeres de Tanzu Kubernetes. Para obtener una plantilla de función de ejemplo que pueda personalizar, consulte Función de ejemplo para la directiva de seguridad de pods. Para obtener un ejemplo sobre cómo restringir el acceso al clúster, consulte https://kubernetes.io/docs/reference/access-authn-authz/rbac/#role-example.

Ejemplos de equilibrador de carga de servicio de Tanzu Kubernetes para la directiva de tráfico local y rangos de IP de origen

Puede configurar un servicio de Kubernetes de tipo LoadBalancer para permitir el tráfico del equilibrador de carga en función de la dirección IP de origen de la solicitud entrante y para permitir únicamente el tráfico del pod local.

Requisitos mínimos

Puede utilizar las funciones `externalTrafficPolicy` y `LoadBalancerSourceRanges` con un servicio de Kubernetes de tipo LoadBalancer en un clúster de Tanzu Kubernetes que cumpla con los siguientes requisitos mínimos:

Componente	Requisito mínimo	Más información
vCenter Server y ESXi	vSphere 7.0 Update 2	Consulte las notas de la versión.
Clúster supervisor	v1.19.1+vmware.2-vsc0.0.8-17610687	Consulte Actualizar clúster supervisor mediante una actualización de los espacios de nombres de vSphere.
Equilibrador de carga	NSX-T Data Center v3.1	Consulte Capítulo 4 Redes para vSphere with Tanzu.
Versión de Tanzu Kubernetes	Una de las versiones más recientes de Tanzu Kubernetes.	Consulte Comprobar la compatibilidad del clúster de Tanzu Kubernetes para actualizar.

Acerca de la compatibilidad con la directiva de tráfico local y los rangos de IP de origen

Si está usando redes de NSX-T Data Center, puede configurar un servicio de Kubernetes de tipo LoadBalancer para permitir la directiva de tráfico externo y rangos de IP de origen del equilibrador de carga. La función `externalTrafficPolicy` permite restringir el tráfico del pod en el nodo local. La función `LoadBalancerSourceRange` permite especificar direcciones IP de origen para permitirlas o bloquearlas.

Servicio de ejemplo para tráfico local solo

La siguiente especificación de servicio del equilibrador de carga configura la instancia del equilibrador de carga con el parámetro `externalTrafficPolicy` establecido en `Local`. El resultado es que el tráfico del pod se enruta solo a esos nodos donde se ejecutan los pods locales.

```
apiVersion: v1
kind: Service
metadata:
  name: local-only
spec:
  selector:
    app: testApp
  ports:
    - protocol: TCP
      port: 80
      targetPort: 80
  externalTrafficPolicy: Local
  type: LoadBalancer
```

La función opera con un monitor de comprobación de estado de NSX-T. Desde una perspectiva de administración de NSX-T, es importante tener en cuenta las operaciones internas de esta función.

Un monitor de comprobación de estado de NSX-T observa el NodePort de comprobación de estado de Kubernetes que asigna kube-proxy para el grupo de servidores que corresponde al servicio de tipo LoadBalancer. El monitor de comprobación de estado de NSX-T envía solicitudes HTTP GET al NodePort de comprobación de estado de destino. El kube-proxy de un nodo devuelve el código de estado HTTP 500 cuando no hay pods locales en ejecución. NSX-T marcará los nodos que no tengan pods locales como DOWN y aparecerán de este modo en NSX Manager. El tráfico se enrutará solo hacia esos nodos que tienen pods locales en ejecución.

Servicio de ejemplo para permitir el tráfico en función de los rangos de IP de origen

La siguiente especificación de servicio del equilibrador de carga configura el parámetro `loadBalancerSourceRanges` con una matriz de CIDR de IP de origen permitidos. Solo se permitirán solicitudes entrantes procedentes de estos rangos de IP de origen y se descartará todo el resto del tráfico entrante.

```
apiVersion: v1
kind: Service
metadata:
  name: allow-based-on-source-IPs
spec:
  selector:
    app: testApp
  ports:
    - protocol: TCP
      port: 80
      targetPort: 80
  loadBalancerSourceRanges:
  - 10.0.0.0/24
  - 10.1.0.0/24
  type: LoadBalancer
```

Ejemplo de entrada de Tanzu Kubernetes mediante Nginx

Un recurso de entrada de Kubernetes proporciona enrutamiento HTTP o HTTPS desde fuera del clúster a uno o varios servicios dentro del clúster. Los clústeres de Tanzu Kubernetes admiten la entrada a través de controladoras de terceros, como Nginx.

En este tutorial, se demuestra cómo implementar un servicio de entrada de Kubernetes basado en Nginx para enrutar el tráfico externo a los servicios en un clúster de Tanzu Kubernetes. Un servicio de entrada requiere una controladora de entrada. Instalamos la controladora de entrada de Nginx con Helm. Helm es un administrador de paquetes para Kubernetes.

Nota Existen varias formas de llevar a cabo esta tarea. Los pasos que se indican a continuación corresponden a un enfoque. Otros enfoques pueden ser más adecuados para su entorno en particular.

Requisitos previos

- Revise el recurso de Entrada en la documentación de Kubernetes.
- Revise la documentación de la controladora de entrada de Nginx.
- Aprovisionar un clúster de Tanzu Kubernetes. Consulte Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS.
- Habilite la directiva de seguridad de pods. Consulte Función de ejemplo para la directiva de seguridad de pods.
- Conectarse al clúster de Tanzu Kubernetes. Consulte Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.

Procedimiento

1 Para instalar Helm, consulte la documentación.

2 Instale la controladora de entrada de Nginx con Helm.

```
helm repo add ingress-nginx https://kubernetes.github.io/ingress-nginx
helm install ingress-nginx ingress-nginx/ingress-nginx
```

3 Compruebe que la controladora de entrada de Nginx esté implementada como un servicio de tipo equilibrador de carga (LoadBalancer).

```
kubectl get services
```

```
NAME                                 TYPE           CLUSTER-IP     EXTERNAL-IP   
PORT(S)                      AGE
ingress-nginx-controller             LoadBalancer   10.16.18.20    10.19.14.76   80:30635/
TCP,443:30873/TCP   59m
ingress-nginx-controller-admission   ClusterIP      10.87.41.25    <none>        
443/TCP                      59m
```

4 Ejecute ping en el equilibrador de carga utilizando la dirección IP externa.

```
ping 10.19.14.76
```

```
Pinging 10.19.14.76 with 32 bytes of data:
Reply from 10.19.14.76: bytes=32 time<1ms TTL=62
Reply from 10.19.14.76: bytes=32 time=1ms TTL=62
```

5 Compruebe que la controladora de entrada de Nginx esté en ejecución.

```
kubectl get pods
```

```
NAME                                        READY   STATUS    RESTARTS   AGE
ingress-nginx-controller-7c6c46898c-v6blt   1/1     Running   0          76m
```

6 Cree un recurso de entrada con una regla de entrada y una ruta de acceso denominada `ingress-hello.yaml`.

```
apiVersion: networking.k8s.io/v1beta1
kind: Ingress
metadata:
  name: ingress-hello
spec:
  rules:
  - http:
      paths:
      - path: /hello
        backend:
          serviceName: hello
          servicePort: 80
```

7 Implemente el recurso `ingress-hello`.

```
kubectl apply -f ingress-hello.yaml
```

```
ingress.networking.k8s.io/ingress-hello created
```

8 Compruebe que el recurso de entrada se haya implementado.

Tenga en cuenta que la dirección IP se asigna a la IP externa de la controladora de entrada.

```
kubectl get ingress
```

```

NAME            CLASS    HOSTS   ADDRESS         PORTS   AGE
ingress-hello   <none>   *       10.19.14.76     80      51m
```

9 Cree una aplicación y un servicio de prueba Hello denominados `ingress-hello-test.yaml`.

```

kind: Service
apiVersion: v1
metadata:
  name: hello
spec:
  selector:
    app: hello
    tier: backend
  ports:
  - protocol: TCP
    port: 80
    targetPort: http
---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: hello
spec:
```

```
  replicas: 3
  selector:
    matchLabels:
      app: hello
      tier: backend
      track: stable
  template:
    metadata:
      labels:
        app: hello
        tier: backend
        track: stable
    spec:
      containers:
        - name: hello
          image: "gcr.io/google-samples/hello-go-gke:1.0"
          ports:
            - name: http
              containerPort: 80
```

10 Implemente el recurso `ingress-hello-test`.

```
kubectl apply -f ingress-hello-test.yaml
```

```

service/hello created
deployment.apps/hello created
```

11 Compruebe que la implementación de `hello` esté disponible.

```
kubectl get deployments
```

```

NAME                       READY   UP-TO-DATE   AVAILABLE   AGE
hello                      3/3     3            3           4m59s
ingress-nginx-controller   1/1     1            1           3h39m
```

12 Obtenga la dirección IP pública del equilibrador de carga que utiliza la controladora de entrada de Nginx.

```
kubectl get ingress
```

```

NAME            CLASS    HOSTS   ADDRESS         PORTS   AGE
ingress-hello   <none>   *       10.19.14.76     80      13m
```

13 Con un navegador, desplácese hasta la dirección IP pública y escriba la ruta de entrada.

```
http://10.19.14.76/hello
```

Se devolverá el mensaje "Hello".

```
{"message":"Hello"}
```

Resultados

El navegador permite acceder externamente a la aplicación de back-end que ofrece el servicio en ejecución dentro del clúster a través de la controladora de entrada con la dirección IP externa del equilibrador de carga.

Ejemplo de clase de almacenamiento de Tanzu Kubernetes

Para las cargas de trabajo que requieren persistencia, puede utilizar la clase de almacenamiento predeterminada o definir su propia clase de almacenamiento para usarla con volúmenes persistentes. Los clústeres de Tanzu Kubernetes admiten el aprovisionamiento de la interfaz de almacenamiento de contenedores (CSI).

Se admite la Interfaz de almacenamiento de contenedor (CSI)

Los clústeres de Tanzu Kubernetes admiten la interfaz de almacenamiento de contenedores (CSI). En la definición de `StorageClass`, este tipo de aprovisionamiento se identifica como `csi.vsphere.vware.com`.

La siguiente definición de YAML se puede utilizar como plantilla a fin de establecer una clase de almacenamiento para un clúster de Tanzu Kubernetes. Especifique si desea que la clase de almacenamiento sea la predeterminada ("true") y proporcione la URL del almacén de datos para el entorno de almacenamiento.

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: tkgs-storage-class
  annotations:
    storageclass.kubernetes.io/is-default-class: "true" or "false"
provisioner: csi.vsphere.vmware.com
parameters:
  datastoreurl: "ds:///vmfs/volumes/vsan:52d8eb4842dbf493-41523be9cd4ff7b7/"
```

Cree la clase de almacenamiento:

```
kubectl apply -f tkgs-storage-class.yaml

storageclass.storage.k8s.io/tkgs-storage-class created
```

Compruebe que se haya creado la clase de almacenamiento:

```
kubectl get storageclass
```

O bien utilice el acceso directo:

```
kubectl get sc
```

No se admite VMware Cloud Provider (vCP)

Los clústeres de Tanzu Kubernetes no admiten el VMware Cloud Provider (vCP) heredado `StorageClass`, como se muestra a continuación. Si intenta crear un `StorageClass` mediante el aprovisionamiento de vCP, no se creará el `StorageClass`.

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: demo-sts-sc
provisioner: kubernetes.io/vsphere-volume
parameters:
  diskformat: thin
```

Ejemplos de notificación de volumen persistente de Tanzu Kubernetes

Para ejecutar cargas de trabajo con estado en clústeres de Tanzu Kubernetes, puede crear una notificación de volumen persistente (Persistent Volume Claim, PVC) para solicitar recursos de almacenamiento persistentes sin conocer los detalles de la infraestructura de almacenamiento subyacente. El almacenamiento que se emplea para la PVC se asigna a partir de la cuota de almacenamiento de espacio de nombres de vSphere.

De forma predeterminada, los contenedores son efímeros y no tienen estado. Para las cargas de trabajo con estado, un método habitual consiste en crear una notificación de volumen persistente (Persistent Volume Claim, PVC). Puede utilizar una PVC para montar los volúmenes persistentes y acceder al almacenamiento. La solicitud aprovisiona dinámicamente un objeto de volumen persistente y un disco virtual coincidente. La notificación está enlazada al volumen persistente. Cuando esta notificación se elimina, se eliminan también el objeto de volumen persistente y el disco virtual aprovisionado correspondientes.

Procedimiento

1 Inicie sesión en el clúster de Tanzu Kubernetes de destino. Consulte Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.

2 Cambie al espacio de nombres en el que se ejecuta el clúster.

```
kubectl config use-context NAMESPACE
```

3 Compruebe la clase de almacenamiento o cree una.

Para comprobar una clase de almacenamiento existente:

```
kubectl get storageclass
```

Para crear una clase de almacenamiento, consulte Ejemplo de clase de almacenamiento de Tanzu Kubernetes.

4 Cree un espacio de nombres.

```
kubectl create namespace guestbook
```

5 Cree los archivos de YAML de la PVC del libro de visitas.

- PVC guía de Redis
- PVC de seguimiento de Redis

6 Aplique las PVC del libro de visitas al clúster.

```
kubectl apply -f redis-leader-pvc.yaml -n guestbook
```

```
kubectl apply -f redis-follower-pvc.yaml -n guestbook
```

7 Compruebe el estado de las PVC.

```
kubectl get pvc,pv -n guestbook
```

Las PVC y los volúmenes persistentes (persistent volumes, PV) se enumeran y están disponibles para su uso.

```
NAME                                       STATUS
VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
AGE
persistentvolumeclaim/redis-follower-pvc   Bound    pvc-37b72f35-3de2-4f84-
be7d-50d5dd968f62   2Gi        RWO            tkgs-storage-class   66s
persistentvolumeclaim/redis-leader-pvc     Bound    pvc-2ef51f31-dd4b-4fe2-bf4c-
f0149cb4f3da   2Gi        RWO            tkgs-storage-class   66s

NAME                                                    CAPACITY   ACCESS MODES   RECLAIM
POLICY STATUS   CLAIM                  STORAGECLASS
persistentvolume/pvc-2ef51f31-dd4b-4fe2-bf4c   2Gi  RWO            Delete
Bound    guestbook/redis-leader-pvc     tkgs-storage-class
persistentvolume/pvc-37b72f35-3de2-4f84-be7d   2Gi  RWO            Delete
Bound    guestbook/redis-follower-pvc   tkgs-storage-class
```

Tutorial del libro de visitas de Tanzu Kubernetes

Implemente la aplicación del libro de visitas en el clúster de Tanzu Kubernetes a fin de explorar la directiva de seguridad de pods para las cuentas de servicio, así como la implementación y la creación de servicios.

La implementación de la aplicación del libro de visitas es un método común para explorar Kubernetes. Si implementa todos los archivos YAML del libro de visitas en un clúster de Tanzu Kubernetes que servicio Tanzu Kubernetes Grid aprovisiona, el pod de la aplicación no se creará correctamente. Aparecerá el siguiente mensaje de error cuando ejecute el comando `kubectl describe pod`:

```
"Error: container has runAsNonRoot and image will run as root"
```

La aplicación del libro de visitas utiliza los recursos `deployment` y `replicaset` para implementar contenedores con privilegios en el espacio de nombres predeterminado. Debido a que la controladora de PodSecurityPolicy está habilitada para los clústeres de Tanzu Kubernetes, cuando un usuario de clúster intenta crear el pod de la aplicación del libro de visitas, las cuentas de servicio de estas controladoras se comprueban con PodSecurityPolicy. Si una PSP adecuada no está enlazada a estas cuentas de servicio, la aplicación no se implementa.

De forma predeterminada, los administradores de Tanzu Kubernetes pueden crear pods con privilegios directamente en cualquier espacio de nombres mediante las cuentas de usuario. Sin embargo, la aplicación del libro de visitas implementa contenedores con privilegios mediante cuentas de servicio. Un administrador de clústeres puede crear los recursos Deployment, StatefulSet y DaemonSet en el espacio de nombres `kube-system`. Sin embargo, la aplicación del libro de visitas implementa estos recursos en el espacio de nombres predeterminado. Asimismo, los usuarios no administrativos no pueden crear pods con o sin privilegios sin los enlaces ni las PSP adecuados.

Una solución consiste en crear enlaces a la PSP con privilegios predeterminada para permitir la implementación de la aplicación del libro de visitas. La instancia de PodSecurityPolicy con privilegios permite pods que se ejecutan como raíz y contenedores con privilegios para cuentas enlazadas. Puede crear un objeto ClusterRoleBinding que aplique `vmware-system-privileged` en todo el clúster. No obstante, esto podría infringir el principio de privilegio mínimo, ya que otorga más permisos de los que se necesita. Un enfoque más apropiado consiste en crear un objeto RoleBinding que permita a las cuentas de servicio del sistema utilizar la instancia de PodSecurityPolicy con privilegios en el espacio de nombres predeterminado. Para obtener más información, consulte Ejemplo de enlaces de funciones para la directiva de seguridad de pods.

Requisitos previos

Revise los siguientes temas:

- Tutorial de la aplicación del libro de visitas en la documentación de Kubernetes
- Usar las directivas de seguridad de pods con clústeres de Tanzu Kubernetes
- Ejemplo de enlaces de funciones para la directiva de seguridad de pods

Procedimiento

1 Inicie sesión en el clúster de Tanzu Kubernetes. Consulte Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.

2 Cree el espacio de nombres del libro de visitas.

```
kubectl create namespace guestbook
```

Compruebe lo siguiente:

```
kubectl get ns
```

3 Cree un control de acceso basado en funciones mediante la instancia de PSP con privilegios predeterminada.

```
kubectl create clusterrolebinding default-tkg-admin-privileged-binding --
clusterrole=psp:vmware-system-privileged --group=system:authenticated
```

Nota Si se requiere una seguridad más estricta, aplique un objeto RoleBinding en el espacio de nombres del libro de visitas. Consulte Ejemplo de enlaces de funciones para la directiva de seguridad de pods.

4 Compruebe la clase de almacenamiento o cree una.

Para comprobar una clase de almacenamiento existente:

```
kubectl get storageclass
```

Para crear una clase de almacenamiento, consulte Ejemplo de clase de almacenamiento de Tanzu Kubernetes.

5 Cree las notificaciones de volumen persistente (persistent volume claims, PVC) que usan la clase de almacenamiento.

Usar los siguientes archivos YAML:

- PVC guía de Redis
- PVC de seguimiento de Redis

Para crear las PVC, consulte Ejemplos de notificación de volumen persistente de Tanzu Kubernetes.

6 Cree los archivos YAML del libro de visitas.

Usar los siguientes archivos YAML:

- Implementación guía de Redis
- Servicio guía de Redis
- Implementación de seguimiento de Redis
- Servicio de seguimiento de Redis
- Implementación de front-end del libro de visitas
- Servicio front-end del libro de visitas

7 Implemente la aplicación del libro de visitas en su espacio de nombres.

```
kubectl apply -f . --namespace guestbook
```

8 Compruebe la creación de los recursos del libro de visitas.

```
kubectl get all -n guestbook
```

```

NAME                                                    READY   STATUS
RESTARTS   AGE
pod/guestbook-frontend-deployment-56fc5b6b47-cd58r   1/1     Running
0          65s
pod/guestbook-frontend-deployment-56fc5b6b47-fh6dp   1/1     Running
0          65s
pod/guestbook-frontend-deployment-56fc5b6b47-hgd2b   1/1     Running
0          65s
pod/redis-follower-deployment-6fc9cf5759-99fgw       1/1     Running
0          65s
pod/redis-follower-deployment-6fc9cf5759-rhxf7       1/1     Running
0          65s
pod/redis-leader-deployment-7d89bbdbcf-flt4q         1/1     Running
0          65s

NAME                                 TYPE           CLUSTER-IP       EXTERNAL-IP
PORT(S)        AGE
service/guestbook-frontend           LoadBalancer   10.10.89.59      10.19.15.99
80:31513/TCP   65s
service/redis-follower               ClusterIP      10.111.163.189   <none>
6379/TCP       65s
service/redis-leader                 ClusterIP      10.111.70.189    <none>
6379/TCP       65s

NAME                                            READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/guestbook-frontend-deployment   3/3     3            3           65s
deployment.apps/redis-follower-deployment       1/2     2            1           65s
deployment.apps/redis-leader-deployment         1/1     1            1           65s

NAME                                                       DESIRED   CURRENT   READY   AGE
replicaset.apps/guestbook-frontend-deployment-56fc5b6b47   3         3         3       65s
replicaset.apps/redis-follower-deployment-6fc9cf5759       2         2         1       65s
replicaset.apps/redis-leader-deployment-7d89bbdbcf         1         1         1       65s
```

9 Acceda a la página web del libro de visitas mediante la dirección `External-IP` del equilibrador de carga de `service/guestbook-frontend` que, en este ejemplo, es `10.19.15.99`.

Puede ver la interfaz web del libro de visitas y puede introducir valores en la base de datos de dicho libro. Si reinicia la aplicación, los datos se conservan.

Archivos YAML de ejemplo para libro de visitas

Utilice los archivos YAML de ejemplo para implementar la aplicación del libro de visitas con datos persistentes.

PVC guía de Redis

El archivo `redis-leader-pvc.yaml` es un ejemplo de notificación de volumen persistente que hace referencia a una clase de almacenamiento con nombre. Para utilizar este ejemplo, introduzca el nombre de la clase de almacenamiento.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: redis-leader-pvc
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: tkgs-storage-class-name
  resources:
    requests:
      storage: 2Gi
```

PVC de seguimiento de Redis

El archivo `redis-follower-pvc.yaml` es un ejemplo de notificación de volumen persistente que hace referencia a una clase de almacenamiento con nombre. Para utilizar este ejemplo, introduzca el nombre de la clase de almacenamiento.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: redis-follower-pvc
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: tkgs-storage-class-name
  resources:
    requests:
      storage: 2Gi
```

Implementación guía de Redis

El archivo `redis-leader-deployment.yaml` es un ejemplo de implementación guía de Redis con un volumen persistente.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: redis-leader-deployment
spec:
  selector:
    matchLabels:
      app: redis
      role: leader
      tier: backend
  replicas: 1
  template:
```

```
    metadata:
      labels:
        app: redis
        role: leader
        tier: backend
    spec:
      containers:
      - name: leader
        image: redis:6.0.5
        resources:
          requests:
            cpu: 100m
            memory: 100Mi
        ports:
        - containerPort: 6379
        volumeMounts:
        - name: redis-leader-data
          mountPath: /data
      volumes:
      - name: redis-leader-data
        persistentVolumeClaim:
          claimName: redis-leader-pvc
```

Implementación de seguimiento de Redis

El archivo `redis-follower-deployment.yaml` es un ejemplo de implementación de seguimiento de Redis con un volumen persistente.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: redis-follower-deployment
  labels:
    app: redis
spec:
  selector:
    matchLabels:
      app: redis
      role: follower
      tier: backend
  replicas: 1
  template:
    metadata:
      labels:
        app: redis
        role: follower
        tier: backend
    spec:
      containers:
      - name: follower
        image: gcr.io/google_samples/gb-redis-follower:v2
        resources:
          requests:
            cpu: 100m
```

```
            memory: 100Mi
        env:
        - name: GET_HOSTS_FROM
          value: dns
        ports:
        - containerPort: 6379
        volumeMounts:
        - name: redis-follower-data
          mountPath: /data
      volumes:
      - name: redis-follower-data
        persistentVolumeClaim:
          claimName: redis-follower-pvc
```

Servicio guía de Redis

El archivo `redis-leader-service.yaml` es un ejemplo de servicio guía de Redis.

```
apiVersion: v1
kind: Service
metadata:
  name: redis-leader
  labels:
    app: redis
    role: leader
    tier: backend
spec:
  ports:
  - port: 6379
    targetPort: 6379
  selector:
    app: redis
    role: leader
    tier: backend
```

Servicio de seguimiento de Redis

El archivo `redis-follower-service.yaml` es un ejemplo de servicio de seguimiento de Redis.

```
apiVersion: v1
kind: Service
metadata:
  name: redis-follower
  labels:
    app: redis
    role: follower
    tier: backend
spec:
  ports:
  - port: 6379
  selector:
    app: redis
    role: follower
    tier: backend
```

Implementación de front-end del libro de visitas

El archivo `guestbook-frontend-deployment.yaml` es un ejemplo de implementación de front-end de un libro de visitas.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: guestbook-frontend-deployment
spec:
  selector:
    matchLabels:
      app: guestbook
      tier: frontend
  replicas: 3
  template:
    metadata:
      labels:
        app: guestbook
        tier: frontend
    spec:
      containers:
      - name: php-redis
        image: gcr.io/google_samples/gb-frontend:v5
        resources:
          requests:
            cpu: 100m
            memory: 100Mi
        env:
        - name: GET_HOSTS_FROM
          value: dns
        ports:
        - containerPort: 80
```

Servicio front-end del libro de visitas

El archivo `guestbook-frontend-service.yaml` es un ejemplo de servicio de equilibrador de carga de front-end de un libro de visitas.

```
apiVersion: v1
kind: Service
metadata:
  name: guestbook-frontend
  labels:
    app: guestbook
    tier: frontend
spec:
  type: LoadBalancer
  ports:
  - port: 80
  selector:
    app: guestbook
    tier: frontend
```

Usar las directivas de seguridad de pods con clústeres de Tanzu Kubernetes

servicio Tanzu Kubernetes Grid aprovisiona clústeres de Tanzu Kubernetes con la controladora de admisión de PodSecurityPolicy habilitada. Esto significa que se requiere la directiva de seguridad de pods para implementar cargas de trabajo. Los administradores de clústeres pueden implementar pods desde su cuenta de usuario a cualquier espacio de nombres y desde cuentas de servicio al espacio de nombres de kube-system. En todos los demás casos prácticos, debe establecer un enlace de manera explícita a un objeto PodSecurityPolicy. Los clústeres incluyen directivas de seguridad de pods predeterminadas a las que se puede enlazar, o bien puede crear una propia.

Acerca de las directivas de seguridad de pods de Kubernetes

Las directivas de seguridad de pods (Pod Security Policy, PSP) de Kubernetes son recursos del nivel del clúster que controlan la seguridad de los pods. Las PSP le permiten controlar los tipos de pods que se pueden implementar y los tipos de cuentas que pueden implementarlos.

Un recurso PodSecurityPolicy define un conjunto de condiciones que un pod debe cumplir para que pueda implementarse. Si no se cumplen las condiciones, el pod no puede implementarse. Un único recurso PodSecurityPolicy debe validar un pod por completo. Algunas de las reglas de un pod no pueden estar en una directiva y algunas de ellas en otra.

Existen varias formas de implementar el uso de directivas de seguridad de pods en Kubernetes. El método habitual consiste en usar objetos de control de acceso basado en funciones (Role-Based Access Control, RBAC). ClusterRole y ClusterRoleBinding se aplican en todo el clúster, mientras que Role y RoleBinding se aplican en un espacio de nombres específico. Si se utiliza RoleBinding, solo permite que los pods se ejecuten en el mismo espacio de nombres que el enlace.

Los pods de Kubernetes pueden crearse de forma directa o indirecta. Un pod se crea de forma directa mediante la implementación de una especificación de pod con la cuenta de usuario. Para crear un pod de forma indirecta, se define un recurso de nivel superior (como Deployment o DaemonSet). En este caso, una cuenta de servicio crea el pod subyacente.

Para utilizar las PSP de forma efectiva, debe tener en cuenta ambos flujos de trabajo de creación de pods. Si un usuario crea un pod de forma directa, la PSP enlazada a la cuenta de usuario controla la operación. Si un usuario crea un pod por medio de una cuenta de servicio, la PSP debe estar enlazada a la cuenta de servicio que se utiliza para crear el pod. Si no se define ninguna cuenta de servicio en la especificación del pod, se utiliza la cuenta de servicio predeterminada del espacio de nombres.

Para obtener más información, consulte Directivas de seguridad de pods, RBAC y Cuentas de servicio en la documentación de Kubernetes.

PodSecurityPolicy predeterminado para clústeres de Tanzu Kubernetes

En la tabla se enumeran y se describen las directivas de seguridad de pods predeterminadas restringidas y con privilegios para los clústeres de Tanzu Kubernetes, así como el objeto ClusterRole predeterminado que se asocia a cada directiva.

Tabla 14-1. Instancia de PodSecurityPolicy predeterminada con objeto ClusterRole asociado

PSP predeterminada	Permiso	Descripción	Objeto ClusterRole predeterminado asociado
`vmware-system-privileged`	**Ejecutar como cualquiera**	PSP permisiva. Equivale a la ejecución de un clúster sin la controladora de admisión de PSP habilitada.	`psp:vmware-system-privileged` puede utilizar esta PSP
`vmware-system-restricted`	**Debe ejecutarse como no raíz**	PSP restrictiva. No permite el acceso con privilegios a los contenedores de pods, bloquea las posibles escalaciones en la raíz y requiere el uso de varios mecanismos de seguridad.	`psp:vmware-system-restricted` puede utilizar esta PSP

No hay enlaces predeterminados para clústeres de Tanzu Kubernetes

El servicio Tanzu Kubernetes Grid no ofrece RoleBinding ni ClusterRoleBinding predeterminados para los clústeres de Tanzu Kubernetes.

Un usuario de vCenter Single Sign-On al que se otorga el permiso **Editar** en un espacio de nombres de vSphere se asigna a la función **cluster-admin** para cualquier clúster de Tanzu Kubernetes implementado en ese espacio de nombres. Un administrador de clústeres autenticado puede usar implícitamente la PSP de `vmware-system-privileged`. Aunque técnicamente no es un ClusterRoleBinding, tiene el mismo efecto.

El administrador de clústeres debe definir los enlaces para permitir o restringir los tipos de pods que los usuarios pueden implementar en un clúster. Si se utiliza un RoleBinding, el enlace solo permite que los pods se ejecuten en el mismo espacio de nombres que el enlace. Esto puede emparejarse con los grupos del sistema para conceder acceso a todos los pods que se ejecutan en el espacio de nombres. Los usuarios que no son administradores y que se autentican en el clúster se asignan a la función `authenticated` y se pueden enlazar a la PSP predeterminada como tal. Consulte Conceder acceso de desarrollador a clústeres de Tanzu Kubernetes.

Efecto del PodSecurityPolicy predeterminado en los clústeres de Tanzu Kubernetes

El siguiente comportamiento se aplica a cualquier clúster de Tanzu Kubernetes:

- Un administrador de clústeres puede crear pods con privilegios directamente en cualquier espacio de nombres mediante su cuenta de usuario.
- Un administrador de clústeres puede crear implementaciones, StatefulSets y DaemonSet (cada uno de los cuales crea pods con privilegios) en el espacio de nombres kube-system. Si desea utilizar un espacio de nombres diferente, consulte Tutorial del libro de visitas de Tanzu Kubernetes.
- Un administrador de clústeres puede crear sus propias PSP (además de las dos PSP predeterminadas) y enlazar estas PSP a cualquier usuario. Si define su propia PSP, consulte Orden de directivas en la documentación de Kubernetes.

- Ningún usuario autenticado puede crear pods con privilegios o sin privilegios hasta que el administrador del clúster enlaza PSP a los usuarios autenticados. Consulte Tutorial del libro de visitas de Tanzu Kubernetes.

Ejemplo de enlaces de funciones para la directiva de seguridad de pods

Los clústeres de Tanzu Kubernetes incluyen PodSecurityPolicy predeterminados a los que se puede enlazar para la implementación de cargas de trabajo con privilegios y restringidas.

Acerca de la directiva de seguridad de pods predeterminada

En esta sección, se proporcionan comandos de YAML y CLI para crear objetos de enlace de funciones a la directiva de seguridad de pods predeterminada, incluidos ClusterRoleBinding y RoleBinding. Para obtener más información, consulte Usar las directivas de seguridad de pods con clústeres de Tanzu Kubernetes.

RoleBinding otorga permisos en un espacio de nombres específico, mientras que ClusterRoleBinding otorga permisos en todo el clúster. La decisión de utilizar RoleBindings o ClusterRoleBinding depende de cada caso práctico. Por ejemplo, si usa ClusterRoleBinding y configura los asuntos para que usen `system:serviceaccounts:<namespace>`, puede enlazar a una PSP antes de que se cree el espacio de nombres. Para obtener más información, consulte RoleBinding y ClusterRoleBinding en la documentación de Kubernetes.

Ejemplo 1: ClusterRoleBinding para ejecutar un conjunto privilegiado de cargas de trabajo

El siguiente comando kubectl crea un ClusterRoleBinding que otorga acceso a los usuarios autenticados para que ejecuten un conjunto de cargas de trabajo con privilegios mediante la PSP predeterminada `vmware-system-privileged`.

Advertencia La aplicación del Ejemplo 1, de forma declarativa o imperativa, permite la implementación de cargas de trabajo con privilegios en todo el clúster. En efecto, el Ejemplo 1 deshabilita los controles de seguridad nativos y debe utilizarse con precaución y con total conocimiento de las implicaciones. Para una seguridad más estricta, considere los Ejemplos 2, 3 y 4.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: psp:privileged
rules:
- apiGroups: ['policy']
  resources: ['podsecuritypolicies']
  verbs:     ['use']
  resourceNames:
  - vmware-system-privileged
---
apiVersion: rbac.authorization.k8s.io/v1
```

```
kind: ClusterRoleBinding
metadata:
  name: all:psp:privileged
roleRef:
  kind: ClusterRole
  name: psp:privileged
  apiGroup: rbac.authorization.k8s.io
subjects:
- kind: Group
  name: system:serviceaccounts
  apiGroup: rbac.authorization.k8s.io
```

Como alternativa a la aplicación de YAML, puede ejecutar el siguiente de comando de `kubectl`:

```
kubectl create clusterrolebinding default-tkg-admin-privileged-binding --
clusterrole=psp:vmware-system-privileged --group=system:authenticated
```

Ejemplo 2: RoleBinding para ejecutar un conjunto de cargas de trabajo con privilegios

El siguiente comando kubectl crea un RoleBinding que otorga acceso a todas las cuentas de servicio dentro del espacio de nombres predeterminado para ejecutar un conjunto de cargas de trabajo con privilegios mediante la PSP predeterminada `vmware-system-privileged`.

```
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: rolebinding-default-privileged-sa-ns_default
  namespace: default
roleRef:
  kind: ClusterRole
  name: psp:vmware-system-privileged
  apiGroup: rbac.authorization.k8s.io
subjects:
- kind: Group
  apiGroup: rbac.authorization.k8s.io
  name: system:serviceaccounts
```

Como alternativa a la aplicación de YAML, puede ejecutar el siguiente de comando de kubectl:

```
kubectl create rolebinding rolebinding-default-privileged-sa-ns_default --namespace=default --
clusterrole=psp:vmware-system-privileged --group=system:serviceaccounts
```

Ejemplo 3: ClusterRoleBinding para ejecutar un conjunto restringido de cargas de trabajo

El siguiente YAML crea un ClusterRoleBinding que otorga a los usuarios autenticados acceso en todo el clúster para ejecutar un conjunto restringido de cargas de trabajo mediante la PSP predeterminada `vmware-system-restricted`.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: psp:authenticated
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:authenticated
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: psp:vmware-system-restricted
```

Como alternativa a la aplicación de YAML, puede ejecutar el siguiente de comando de kubectl:

```
kubectl create clusterrolebinding psp:authenticated --clusterrole=psp:vmware-system-
restricted --group=system:authenticated
```

Ejemplo 4: RoleBinding para ejecutar un conjunto restringido de cargas de trabajo

El siguiente YAML crea un RoleBinding que otorga acceso a todas las cuentas de servicio dentro de un espacio de nombres específico para ejecutar un conjunto restringido de cargas de trabajo mediante la PSP predeterminada `vmware-system-restricted`.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: psp:serviceaccounts
  namespace: some-namespace
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:serviceaccounts
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: psp:vmware-system-restricted
```

Como alternativa a la aplicación de YAML, puede ejecutar el siguiente de comando de kubectl:

```
kubectl create rolebinding psp:serviceaccounts --clusterrole=psp:vmware-system-restricted --
group=system:serviceaccounts
```

Función de ejemplo para la directiva de seguridad de pods

Los clústeres de Tanzu Kubernetes requieren una directiva de seguridad de pods (Pod Security Policy, PSP) para implementar cargas de trabajo. Si define su propia PSP, debe crear una función o ClusterRole que haga referencia a la PSP.

Función de ejemplo para PodSecurityPolicy

El siguiente ejemplo demuestra una función enlazada a PodSecurityPolicy. En la definición de la función, la función `example-role` otorgada al verbo `use` para un recurso de PSP personalizado que usted defina. De forma alternativa, utilice una de las PSP predeterminadas. A continuación, cree un Tutorial del libro de visitas de Tanzu Kubernetes.

```
apiVersion: rbac.authorization.k8s.io/v1beta1
kind: Role
metadata:
  name: example-role
  namespace: tkgs-cluster-ns
rules:
- apiGroups:
  - ""
  resources:
  - configmaps
  verbs:
  - create
  - get
  - list
  - watch
  - update
- apiGroups:
  - ""
  resources:
  - events
  verbs:
  - create
  - update
  - patch
- apiGroups:
  - extensions
  resourceNames:
  - CUSTOM-OR-DEFAULT-PSP
  resources:
  - podsecuritypolicies
  verbs:
  - use
```

Implementar paquetes TKG en clústeres de Tanzu Kubernetes

Consulte este conjunto de instrucciones para implementar paquetes TKG en clústeres de Tanzu Kubernetes aprovisionados por TKGS.

Paquetes de TKG 1.6

Para instalar paquetes de TKG 1.6 en los clústeres de Tanzu Kubernetes aprovisionados por TKGS, consulte Instalar y configurar paquetes de TKG 1.6.

Paquetes de TKG 1.4

Para instalar paquetes de TKG 1.4 en los clústeres de Tanzu Kubernetes aprovisionados por TKGS, consulte Instalar y configurar paquetes de TKG 1.4.

Extensiones TKG 1.3.1

Para instalar extensiones TKG 1.3.1 en los clústeres de Tanzu Kubernetes aprovisionados por TKGS, consulte la documentación de esta sección.

Nota Los paquetes de TKG reemplazan a las extensiones de TKG. Considere la posibilidad de utilizar paquetes en lugar de extensiones.

Descargar el paquete de extensiones TKG v1.3.1

Para preparar la implementación de una o varias extensiones TKG, descargue el paquete de extensiones TKG v1.3.1 desde VMware.

Las extensiones TKG se empaquetan como un paquete independiente que se descarga de VMware.

Nota vSphere with Tanzu es compatible con las extensiones TKG v1.3.1 en vSphere 7 U2 y versiones posteriores.

Procedimiento

1 Vaya a https://www.vmware.com/go/get-tkg.

2 Inicie sesión con sus credenciales de My VMware.

3 Seleccione **Descargas de productos > Ir a descargas**.

4 Seleccione la versión **1.3.1** en el menú desplegable.

5 Desplácese hasta **VMware Tanzu Kubernetes Grid Extensions Manifest 1.3.1** y localícelo.

6 Haga clic en **Descargar ahora** para descargar el archivo `tkg-extensions-manifests-v1.3.1-vmware.1.tar.gz` en el sistema local.

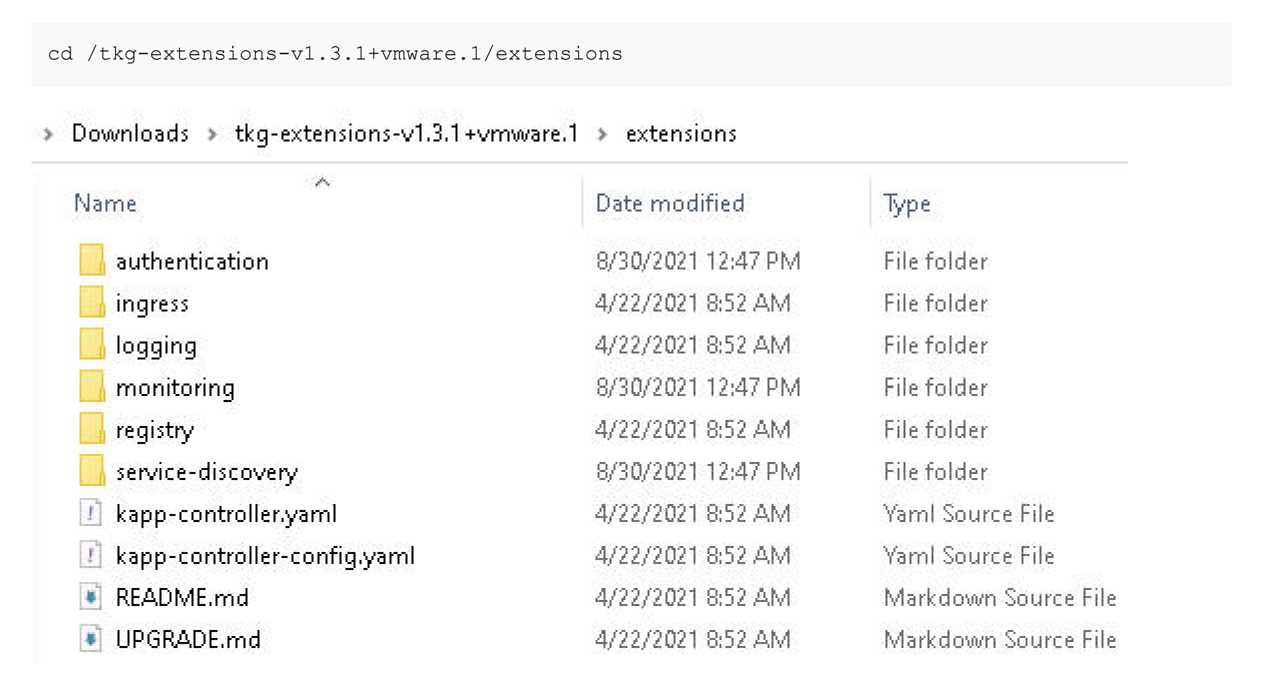
7 Copie el archivo `tkg-extensions-manifests-v1.3.1-vmware.1.tar.gz` en el equipo donde ejecuta los comandos `kubectl`.

8 Mediante el comando `tar` o la herramienta de extracción que elija, extraiga los archivos de las extensiones TKG.

```
tar -xzf tkg-extensions-manifests-v1.3.1-vmware.1.tar.gz
```

9 Para comprobar los archivos de las extensiones TKG, vaya a la siguiente ruta de archivo.

```
cd /tkg-extensions-v1.3.1+vmware.1/extensions
```



Este es el directorio inicial de las extensiones TKG.

Instalar los requisitos previos de las extensiones TKG

Instale las aplicaciones de requisitos previos en cada clúster de Tanzu Kubernetes en el que tiene pensado instalar una o varias extensiones TKG v1.3.1.

Las extensiones TKG v1.3.1 requieren dos componentes de requisitos previos: controladora Kapp y administrador de certificados.

Nota Como alternativa al administrador de certificados, puede utilizar sus propios certificados TLS. Consulte Utilizar su propio certificado TLS en extensiones de TKG.

Requisitos previos

- Aprovisionar un clúster de Tanzu Kubernetes. Consulte Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS.
- Conectarse al clúster de Tanzu Kubernetes. Consulte Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.

Procedimiento

1 Descargar el paquete de extensiones TKG v1.3.1.

2 Instale el administrador de certificados en el clúster.

Desplácese hasta el directorio raíz del paquete de extensiones TKG que descargó y extrajo.

```
cd /tkg-extensions-v1.3.1+vmware.1
```

El administrador de certificados incluye varios componentes. Hay tres archivos YAML en el directorio denominado `/cert-manager`. Utilice `ls` para comprobar la presencia de este directorio.

Instale todos los componentes del administrador de certificados mediante el siguiente comando único:

```
kubectl apply -f cert-manager/
```

Esta operación crea el espacio de nombres `cert-manager`, los componentes, los certificados y los objetos asociados.

3 Instale la controladora Kapp en el clúster.

La controladora Kapp se instala mediante `kapp-controller.yaml`. Si fuera necesario, puede personalizar la configuración de la controladora Kapp mediante `kapp-controller-config.yaml`.

Desplácese hasta el directorio principal de las extensiones TKG.

```
cd /tkg-extensions-v1.3.1+vmware.1/extensions
```

Utilice `ls` para comprobar la presencia de archivos de la controladora Kapp `kapp-controller.yaml` y `kapp-controller-config.yaml`.

El contenedor de la controladora Kapp se instala con los parámetros de configuración predeterminados. Por lo general, puede instalar la controladora Kapp sin personalizar la configuración. Si necesita personalizar la controladora Kapp, edite el `kapp-controller-config.yaml`. Por ejemplo, tendrá que editar este archivo si va a implementar la controladora Kapp detrás de un proxy.

Si fuera necesario, edite el archivo `kapp-controller-config.yaml`. Si edita el archivo de configuración, guárdelo y aplique los cambios mediante el siguiente comando.

```
kubectl apply -f kapp-controller-config.yaml
```

El contenedor de la controladora Kapp se instala mediante el archivo `kapp-controller.yaml`. La ruta `spec.containers.image` de este archivo YAML apunta al registro de VMware público. En instalaciones aisladas, actualice esta ruta de acceso para que apunte a su registro privado.

Ejecute el siguiente comando para instalar la controladora Kapp.

```
kubectl apply -f kapp-controller.yaml
```

Esta operación crea el espacio de nombres `tkg-system`, la aplicación kapp-controller y los objetos de función.

4 Compruebe la instalación del administrador de certificados y la controladora Kapp.

Ejecute el comando `kubectl get pods -A`. Debería ver que todos ellos están en ejecución.

```
cert-manager       cert-manager-cainjector-...    1/1     Running    0      7h54m
cert-manager       cert-manager-...               1/1     Running    0      7h54m
cert-manager       cert-manager-webhook-...       1/1     Running    0      7h54m
tkg-system         kapp-controller-...            1/1     Running    0      16m
```

Revisar los requisitos previos de almacenamiento persistente para las extensiones de TKG

Las dos extensiones de supervisión, Prometheus y Grafana, requieren un almacenamiento persistente. Para preparar la implementación de estas extensiones, compruebe que el clúster de Tanzu Kubernetes de destino esté configurado con una clase de almacenamiento predeterminada y que el espacio de nombres de vSphere tenga suficiente almacenamiento.

Requisitos de almacenamiento persistente para las extensiones de TKG

El clúster de Tanzu Kubernetes donde se implementan las extensiones Prometheus o Grafana debe aprovisionarse con una clase de almacenamiento predeterminada. Consulte Ejemplos del aprovisionamiento de clústeres de Tanzu Kubernetes mediante la API de servicio Tanzu Kubernetes Grid v1alpha1.

Como alternativa, puede configurar las extensiones para que usen una notificación de volumen persistente cuando las implemente. Puede encontrar la configuración de esta opción en las instrucciones de implementación de cada extensión.

El límite de almacenamiento del espacio de nombres de vSphere en el que se aprovisiona el clúster donde se va a instalar la extensión debe ser mayor que el tamaño total de las notificaciones de volumen persistente.

Tabla 14-2. Requisitos de almacenamiento predeterminados para las extensiones de TKG

Componente	Extensión TKG	Tamaño de almacenamiento predeterminado
Grafana	Grafana	8 Gi
Servidor Prometheus	Prometheus	8 Gi
Administrador de alertas	Prometheus	8 Gi
Harbor	Registro de Harbor	Varía según la PVC

Ajustar el límite de almacenamiento del espacio de nombres de vSphere

Para ajustar el límite de almacenamiento del espacio de nombres de vSphere donde se aprovisiona el clúster de Tanzu Kubernetes:

1. Con vSphere Client, inicie sesión en la instancia de vCenter Server en la que está habilitado vSphere with Tanzu.
2. Seleccione el espacio de nombres de vSphere donde se aprovisiona el clúster de Tanzu Kubernetes de destino.
3. Seleccione **Configurar > Límites de recursos**.
4. Haga clic en **Editar**.
5. Ajuste el límite de **Almacenamiento** para que sea mayor que el tamaño total de las notificaciones de volumen persistente que se requieren para las extensiones Prometheus y Grafana.

Utilizar su propio certificado TLS en extensiones de TKG

Las extensiones de TKG requieren certificados TLS. Puede instalar cert-manager para cumplir con este requisito previo o puede utilizar sus propios certificados autofirmados. También se admiten certificados de una entidad de certificación (CA).

Acerca del uso de sus propios certificados TLS con extensiones de TKG

La instalación de cert-manager está documentada como parte del proceso de implementación de cada extensión de TKG. Si lo desea, puede utilizar sus propios certificados TLS.

Nota En esta tarea, se asume que utilizará un host de Linux con OpenSSL instalado.

Generar un certificado de entidad de certificación

En un entorno de producción, debe obtener un certificado de una CA. En un entorno de prueba o desarrollo, puede generar su propio certificado autofirmado. Para generar un certificado de CA, siga estas instrucciones.

1. Genere una clave privada de un certificado de CA.

   ```
   openssl genrsa -out ca.key 4096
   ```

2. Genere el certificado de CA.

   Utilice el siguiente comando como plantilla. Actualice los valores en la opción `-subj` en función de su entorno. Si utiliza un FQDN para conectar el host de las extensiones de TKG, debe especificar este FQDN como el atributo de nombre común (CN).

   ```
   openssl req -x509 -new -nodes -sha512 -days 3650 \
    -subj "/C=US/ST=PA/L=PA/O=example/OU=Personal/CN=tkg-extensions.system.tanzu" \
    -key ca.key \
    -out ca.crt
   ```

Generar un certificado de servidor

Por lo general, el certificado contiene un archivo .crt y un archivo .key, por ejemplo, `tls.crt` y `tls.key`.

1 Genere una clave privada.

```
openssl genrsa -out tls.key 4096
```

2 Genere una solicitud de firma del certificado (CSR).

Utilice el siguiente comando como plantilla. Actualice los valores en la opción `-subj` en función de su entorno. Si utiliza un FQDN para conectar el host de las extensiones de TKG, debe especificar este FQDN como el atributo de nombre común (CN) y utilizar el FQDN en los nombres de archivo de la CSR y la clave.

```
openssl req -sha512 -new \
    -subj "/C=US/ST=PA/L=PA/O=example/OU=Personal/CN=tkg-extensions.system.tanzu" \
    -key tls.key \
    -out tls.csr
```

3 Genere un archivo de extensión x509 v3.

Utilice el siguiente comando como plantilla. Cree este archivo de modo que pueda generar un certificado para el host de las extensiones de TKG que cumpla con los requisitos de extensión de nombre alternativo del firmante (SAN) y de extensión x509 v3.

```
cat > v3.ext <<-EOF
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names

[alt_names]
DNS.1=tkg-extensions.system.tanzu
EOF
```

4 Utilice el archivo de extensión x509 v3 a fin de generar un certificado para el host de extensiones de TKG

```
openssl x509 -req -sha512 -days 3650 \
-extfile v3.ext \
-CA ca.crt -CAkey ca.key -CAcreateserial \
-in tls.csr \
-out tls.crt
```

5 Copie el contenido de los archivos `ca.crt`, `tls.crt` y `tls.key` en el archivo `TKG-EXTENSION-data-values.yaml` usando el siguiente formato.

```
ingress:
  tlsCertificate:
    tls.crt: |
        -----BEGIN ...
```

6 Continúe con la implementación de una extensión de TKG compatible del modo en que se documenta.

Implementar y administrar la extensión TKG para el registro de Fluent Bit

En este tema se describe cómo implementar la extensión TKG v1.3.1 para Fluent Bit. Fluent Bit es un reenviador y procesador de registros rápido y ligero que le permite recopilar registros y datos de aplicaciones de diferentes orígenes, así como unificarlos y enviarlos a varios destinos. Implemente la extensión TKG para que Fluent Bit recopile y reenvíe registros de clústeres de Tanzu Kubernetes al destino de su elección.

Requisitos previos de la extensión

Cumpla los siguientes requisitos antes de implementar la extensión TKG v1.3.1 para Fluent Bit.

- Aprovisionar un clúster. Consulte Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS.
- Conéctese al clúster. Consulte Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.
- Descargar el paquete de extensiones TKG v1.3.1 Al host cliente en el que se ejecuta kubectl.
- Instalar los requisitos previos de las extensiones TKG en el clúster de destino.

Implementar la extensión Fluent Bit

La extensión TKG para Fluent Bit instala un contenedor de Fluent Bit en el clúster. Para obtener más información sobre este contenedor, consulte https://fluentbit.io/.

Contenedor	Tipo de recurso	Réplicas	Descripción
Fluent Bit	DaemonSet	6	Recopilador de registros, agregador, reenviador

La extensión está configurada para extraer los contenedores del registro público de VMware en https://projects.registry.vmware.com/. Si utiliza un registro privado, cambie la URL del endpoint en los valores de datos y los archivos de las configuraciones de extensión para que coincidan. Consulte Configurar la extensión Fluent Bit para ver una descripción de los campos y las opciones.

1 Compruebe que completó cada uno de los requisitos previos de extensión. Consulte Requisitos previos de la extensión.

2 Cambie el directorio a la extensión Fluent Bit.

```
cd /tkg-extensions-v1.3.1+vmware.1/extensions/logging/fluent-bit
```

3 Cree el espacio de nombres `tanzu-system-logging`, así como los objetos de función y la cuenta de servicio de Fluent Bit.

```
kubectl apply -f namespace-role.yaml
```

4 Decida qué destino de registro utilizará para Fluent Bit. Entre los resultados admitidos se incluyen Elasticsearch, HTTP, Kafka, Splunk y Syslog. Consulte https://docs.fluentbit.io/manual/pipeline/outputs para obtener más información.

5 Cree un archivo de valores de datos de Fluent Bit para el destino de registro elegido copiando uno de los archivos `<LOG_BACKEND>/fluent-bit-data-values.example.yaml`.

Hay un archivo de valores de datos de ejemplo para cada destino de registro compatible. El ejemplo proporciona la configuración mínima para ese destino de registro.

```
cp elasticsearch/fluent-bit-data-values.yaml.example elasticsearch/fluent-bit-data-
values.yaml
```

```
cp http/fluent-bit-data-values.yaml.example http/fluent-bit-data-values.yaml
```

```
cp kafka/fluent-bit-data-values.yaml.example kafka/fluent-bit-data-values.yaml
```

```
cp splunk/fluent-bit-data-values.yaml.example splunk/fluent-bit-data-values.yaml
```

```
cp syslog/fluent-bit-data-values.yaml.example syslog/fluent-bit-data-values.yaml
```

6 Configure la extensión Fluent Bit. Para ello, rellene `<LOG_BACKEND>/fluent-bit-data-values.yaml`. Consulte Configurar la extensión Fluent Bit para ver una descripción de los campos y las opciones.

Por ejemplo, la configuración de syslog de Fluent Bit requiere los siguientes valores:

```
logging:
  image:
    repository: projects.registry.vmware.com/tkg # Public registry
tkg:
  instance_name: "<TKG_INSTANCE_NAME>" #mandatory but arbitrary; appears in logs
  cluster_name: "<CLUSTER_NAME>" #name of the target tkgs cluster
fluent_bit:
  output_plugin: "syslog"
  syslog:
    host: "<SYSLOG_HOST>"
    port: "<SYSLOG_PORT>"
    mode: "<SYSLOG_MODE>"
    format: "<SYSLOG_FORMAT>"
```

Un archivo de valores de datos rellenado para syslog de Fluent Bit podría tener la siguiente configuración:

```
logging:
  image:
    repository: projects.registry.vmware.com/tkg
tkg:
  instance_name: "tkgs-cluster-1"
  cluster_name: "tkgs-cluster-1"
fluent_bit:
  output_plugin: "syslog"
  syslog:
    host: "10.192.175.59"
    port: "514"
    mode: "tcp"
    format: "rfc5424"
```

7 Cree un secreto de Fluent Bit con valores de datos para el destino de registro.

```
kubectl create secret generic fluent-bit-data-values --from-file=values.yaml=elasticsearch/
fluent-bit-data-values.yaml -n tanzu-system-logging
```

```
kubectl create secret generic fluent-bit-data-values --from-file=values.yaml=kafka/fluent-
bit-data-values.yaml -n tanzu-system-logging
```

```
kubectl create secret generic fluent-bit-data-values --from-file=values.yaml=splunk/fluent-
bit-data-values.yaml -n tanzu-system-logging
```

```
kubectl create secret generic fluent-bit-data-values --from-file=values.yaml=http/fluent-
bit-data-values.yaml -n tanzu-system-logging
```

```
kubectl create secret generic fluent-bit-data-values --from-file=values.yaml=syslog/fluent-
bit-data-values.yaml -n tanzu-system-logging
```

`secret/fluent-bit-data-values` se crea en el espacio de nombres `tanzu-system-logging`. Verifique con el siguiente comando:

```
kubectl get secrets -n tanzu-system-logging
```

8 Implemente la aplicación Fluent Bit.

```
kubectl apply -f fluent-bit-extension.yaml
```

Si todo es correcto, debería ver `app.kappctrl.k14s.io/fluent-bit created`.

9 Compruebe el estado de la aplicación Fluent Bit.

```
kubectl get app fluent-bit -n tanzu-system-logging
```

Si es correcto, el estado debe cambiar de `Reconciling` a `Reconcile succeeded`. Si el estado es `Reconcile failed`, consulte Solucionar problemas generados en la implementación de Fluent Bit.

10 Vea el estado detallado de la aplicación.

```
kubectl get app fluent-bit -n tanzu-system-logging -o yaml
```

11 Compruebe el DaemonSet de Fluent Bit.

```
kubectl get daemonsets -n tanzu-system-logging
```

Si es correcto, debería ver lo siguiente:

```
NAME         DESIRED   CURRENT   READY   UP-TO-DATE   AVAILABLE   NODE SELECTOR   AGE
fluent-bit   6         6         6       6            6           <none>          105s
```

Solucionar problemas generados en la implementación de Fluent Bit

Si se produce un error en la implementación o la reconciliación, ejecute `kubectl get pods -A` para ver el estado del pod. Los pods de `fluent-bit` deben tener el estado `Running`. Si el estado de un pod es `ImagePullBackOff` o `ImageCrashLoopBackOff`, no se podrá extraer la imagen del contenedor. Compruebe la URL del registro en los valores de datos y los archivos YAML de extensión, y asegúrese de que sean precisos.

Compruebe los registros del contenedor, donde `name-XXXX` es el nombre único del pod que puede ver cuando ejecuta `kubectl get pods -A`:

```
kubectl logs pod/fluent-bit-XXXXX -c fluent-bit -n tanzu-system-logging
```

Actualizar la extensión de Fluent Bit

Actualice la extensión de Fluent Bit que está implementada en el clúster de Tanzu Kubernetes.

1 Obtenga los valores de datos de Fluent Bit del secreto.

```
kubectl get secret fluent-bit-data-values -n tanzu-system-logging -o 'go-
template={{ index .data "values.yaml" }}' | base64 -d > fluent-bit-data-values.yaml
```

2 Actualice los valores de datos de Fluent Bit en `fluent-bit-data-values.yaml`. Consulte Configurar la extensión Fluent Bit.

3 Actualice el secreto de los valores de datos de Fluent Bit.

```
kubectl create secret generic fluent-bit-data-values --from-file=values.yaml=fluent-bit-
data-values.yaml -n tanzu-system-logging -o yaml --dry-run | kubectl replace -f-
```

La extensión de Fluent Bit se conciliará de nuevo con los valores de datos anteriores.

Nota De forma predeterminada, kapp-controller sincronizará las aplicaciones cada 5 minutos. La actualización debería tener efecto en 5 minutos o menos. Si desea que la actualización se aplique inmediatamente, cambie los valores de `syncPeriod` en `fluent-bit-extension.yaml` a un valor menor y aplique la extensión de Fluent Bit mediante `kubectl apply -f fluent-bit-extension.yaml`.

4 Compruebe el estado de la extensión.

```
kubectl get app fluent-bit -n tanzu-system-logging
```

5 Vea el estado detallado y solucione los problemas.

```
kubectl get app fluent-bit -n tanzu-system-logging -o yaml
```

6 Solucione los problemas en caso necesario. Consulte Solucionar problemas generados en la implementación de Fluent Bit.

Eliminar la extensión Fluent Bit

Elimine la extensión Fluent Bit de un clúster de Tanzu Kubernetes.

Nota Complete los pasos en orden. No elimine el espacio de nombres, la cuenta de servicio ni los objetos de función antes de eliminar totalmente la aplicación Fluent Bit. De lo contrario, podría provocar errores en el sistema.

1 Cambie el directorio a la extensión Fluent Bit.

```
cd extensions/logging/fluent-bit/
```

2 Elimine la aplicación Fluent Bit.

```
kubectl delete app fluent-bit -n tanzu-system-logging
```

Resultado esperado: `app.kappctrl.k14s.io "fluent-bit" deleted`.

3 Compruebe que el aplicación Fluent Bit se haya eliminado.

```
kubectl get app fluent-bit -n tanzu-system-logging
```

Resultado esperado: `apps.kappctrl.k14s.io "fluent-bit" not found`.

4 Elimine el espacio de nombres `tanzu-system-logging`, así como los objetos de función y la cuenta de servicio de la extensión Fluent Bit.

```
kubectl delete -f namespace-role.yaml
```

Actualizar la extensión de Fluent Bit

Si tiene una extensión de Fluent Bit existente implementada, puede actualizarla a la versión más reciente.

1 Exporte el mapa de configuración de Fluent Bit.

```
kubectl get configmap fluent-bit -n tanzu-system-logging -o 'go-template={{ index .data
"fluent-bit.yaml" }}' > fluent-bit-configmap.yaml
```

2 Elimine la implementación existente de Fluent Bit. Consulte Eliminar la extensión Fluent Bit.

3 Implemente la última extensión Fluent Bit. Consulte Implementar la extensión Fluent Bit.

Configurar la extensión Fluent Bit

Los valores de configuración se establecen en `extensions/logging/fluent-bit/<LOG_BACKEND>/fluent-bit-data-values.yaml`.

Tabla 14-3. Configuraciones de extensión de Fluent Bit

Parámetro	Descripción	Tipo	Predeterminado
logging.namespace	Espacio de nombres en el que se implementará Fluent Bit	string	tanzu-system-logging
logging.service_account_name	Nombre de la cuenta del servicio Fluent Bit	string	fluent-bit
logging.cluster_role_name	Nombre de la función de clúster que otorga permisos para obtener, ver y enumerar Fluent Bit	string	fluent-bit-read
logging.image.name	Nombre de la imagen de Fluent Bit	string	fluent-bit
logging.image.tag	Etiqueta de la imagen de Fluent Bit. Es posible que este valor tenga que actualizarse si va a actualizar la versión.	string	v1.6.9_vmware.1
logging.image.repository	Ubicación del repositorio con la imagen de Fluent Bit. El valor predeterminado es el registro de VMware público. Cambie este valor si utiliza un repositorio privado (p. ej., un entorno aislado).	string	projects.registry.vmware.com/tkg
logging.image.pullPolicy	Directiva de extracción de imágenes de Fluent Bit	string	IfNotPresent
logging.update_strategy	Estrategia de actualización que se utilizará al actualizar DaemonSet	string	RollingUpdate

Tabla 14-3. Configuraciones de extensión de Fluent Bit (continuación)

Parámetro	Descripción	Tipo	Predeterminado
tkg.cluster_name	Nombre del clúster de Tanzu Kubernetes	string	Nulo (parámetro obligatorio)
tkg.instance_name	Nombre definido por el usuario de la instancia de TKG compartida por el clúster supervisor y todos los clústeres de Tanzu Kubernetes en una implementación. Puede utilizar cualquier nombre relacionado con la instalación.	string	Nulo (parámetro obligatorio) **Nota** Este campo es obligatorio pero arbitrario. Es un nombre que aparece en los registros.
fluent_bit.log_level	Nivel de registro que se utilizará para Fluent Bit	string	info
fluent_bit.output_plugin	Establezca el back-end en el que Fluent Bit debería vaciar la información que recopila	string	Nulo (parámetro obligatorio)
fluent_bit.elasticsearch.host	Dirección IP o nombre de host de la instancia Elasticsearch de destino	string	Nulo (parámetro obligatorio cuando output_plugin es una búsqueda elástica)
fluent_bit.elasticsearch.port	Puerto TCP de la instancia Elasticsearch de destino	entero	Nulo (parámetro obligatorio cuando output_plugin es una búsqueda elástica)
fluent_bit.elasticsearch.buffer_size	Especifique el tamaño de búfer utilizado para leer la respuesta del servicio Elasticsearch. Se establece en ilimitado si es False	string	False
fluent_bit.elasticsearch.tls	Especifique la configuración predeterminada de TLS para Elasticsearch	string	Desactivado
fluent_bit.kafka.broker_service_name	Lista única o múltiple de Kafka Brokers; por ejemplo, 192.168.1.3:9092	string	Nulo (parámetro obligatorio cuando output_plugin es kafka)
fluent_bit.kafka.topic_name	Entrada única o lista de temas separados por (,) que Fluent Bit usará para enviar mensajes a Kafka	string	Nulo (parámetro obligatorio cuando output_plugin es kafka)
fluent_bit.splunk.host	Dirección IP o nombre de host del servidor Splunk de destino	string	Nulo (parámetro obligatorio cuando output_plugin es splunk)
fluent_bit.splunk.port	Puerto TCP del servidor Splunk de destino	entero	Nulo (parámetro obligatorio cuando output_plugin es splunk)

Tabla 14-3. Configuraciones de extensión de Fluent Bit (continuación)

Parámetro	Descripción	Tipo	Predeterminado
fluent_bit.splunk.token	Especifica el token de autenticación de la interfaz del recopilador de eventos HTTP	string	Nulo (parámetro obligatorio cuando output_plugin es splunk)
fluent_bit.http.host	Dirección IP o nombre de host del servidor HTTP de destino	string	Nulo (parámetro obligatorio cuando output_plugin es http)
fluent_bit.http.port	Puerto TCP del servidor HTTP de destino	entero	Nulo (parámetro obligatorio cuando output_plugin es http)
fluent_bit.http.mode	Especificar un URI HTTP para el servidor web de destino	string	Nulo (parámetro obligatorio cuando output_plugin es http)
fluent_bit.http.header_key_value	Par clave/valor de encabezado HTTP. Se pueden establecer varios encabezados	string	Nulo (parámetro obligatorio cuando output_plugin es http)
fluent_bit.http.format	Especifica el formato de datos que se utilizará en el cuerpo de la solicitud HTTP	string	Nulo (parámetro obligatorio cuando output_plugin es http)
fluent_bit.syslog.host	Dominio o dirección IP del servidor Syslog remoto	string	Nulo (parámetro obligatorio cuando output_plugin es syslog)
fluent_bit.syslog.port	Puerto TCP o UDP del servidor Syslog remoto	entero	Nulo (parámetro obligatorio cuando output_plugin es syslog)
fluent_bit.syslog.mode	Especifique el tipo de transporte de TCP, UDP y TLS	string	Nulo (parámetro obligatorio cuando output_plugin es syslog)
fluent_bit.syslog.format	Especifica el formato de datos que se utilizará en el cuerpo de la solicitud HTTP	string	Nulo (parámetro obligatorio cuando output_plugin es syslog)
host_path.volume_1	Ruta de directorio desde el sistema de archivos del nodo host hacia el pod, para el volumen 1	string	/var/log
host_path.volume_2	Ruta de directorio desde el sistema de archivos del nodo host hacia el pod, para el volumen 2	string	/var/lib/docker/containers

Tabla 14-3. Configuraciones de extensión de Fluent Bit (continuación)

Parámetro	Descripción	Tipo	Predeterminado
host_path.volume_3	Ruta de directorio desde el sistema de archivos del nodo host hacia el pod, para el volumen 3	string	/run/log
systemd.path	Ruta de acceso al directorio de diario Systemd	string	/var/log/journal

Implementar y administrar la extensión TKG para la entrada de Contour

En este tema se describe cómo implementar la extensión TKG v1.3.1 para la entrada de Contour. Contour es un controlador de entrada de Kubernetes que utiliza el proxy inverso Envoy. Implemente la extensión TKG para la entrada de Contour a la hora de exponer las rutas de entrada a los servicios que se ejecutan en los clústeres de Tanzu Kubernetes.

Requisitos previos de la extensión

Cumpla los siguientes requisitos para implementar la extensión TKG v1.3.1 para la entrada de Contour.

- Aprovisionar un clúster. Consulte Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS.
- Conéctese al clúster. Consulte Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.
- Descargar el paquete de extensiones TKG v1.3.1 Al host cliente en el que se ejecuta kubectl.
- Instalar los requisitos previos de las extensiones TKG en el clúster de destino.

Implementar la extensión Contour

La extensión TKG para la entrada de Contour instala dos contenedores en el clúster: Envoy y Contour. Para obtener más información, consulte https://projectcontour.io/.

Contenedor	Tipo de recurso	Réplicas	Descripción
Envoy	DaemonSet	3	Proxy inverso de alto rendimiento
Contour	Implementación	2	Servidor de administración y configuración para Envoy

La extensión está configurada para extraer los contenedores del registro público de VMware en https://projects.registry.vmware.com/. Si utiliza un registro privado, cambie la URL del endpoint en los valores de datos y las configuraciones de extensión para que coincidan. Consulte Configurar la extensión Contour.

1 Asegúrese de haber completado cada uno de los requisitos previos de la extensión. Consulte Requisitos previos de la extensión.

2 Cambie el directorio en el que descargó los archivos de la extensión Contour.

```
cd /tkg-extensions-v1.3.1+vmware.1/extensions/ingress/contour
```

3 Ejecute el siguiente comando para crear el espacio de nombres `tanzu-system-ingress`, así como los objetos de función y la cuenta de servicio de Contour.

```
kubectl apply -f namespace-role.yaml
```

4 Cree un archivo de valores de datos de Contour para vSphere.

```
cp vsphere/contour-data-values-lb.yaml.example vsphere/contour-data-values.yaml
```

5 Para configurar Contour, actualice el archivo `vsphere/contour-data-values.yaml`.

El archivo de valores de datos de ejemplo proporciona la configuración mínima requerida. Consulte Configurar la extensión Contour para ver una descripción de todos los campos y las opciones de configuración.

Por ejemplo, la siguiente configuración de Contour para vSphere utiliza un servicio de tipo LoadBalancer.

```
infrastructure_provider: "vsphere"
contour:
  image:
    repository: projects.registry.vmware.com/tkg
envoy:
  image:
    repository: projects.registry.vmware.com/tkg
    tag: v1.17.3_vmware.1
  service:
    type: "LoadBalancer"
```

Nota Se recomienda especificar la versión de imagen de Envoy `v1.17.3_vmware.1` para no utilizar la versión de imagen de Envoy `v1.16.2_vmware.1`, la cual tiene un CVE. Para obtener más información, consulte las Notas de la versión.

6 Cree un secreto con los valores de datos.

```
kubectl create secret generic contour-data-values --from-file=values.yaml=vsphere/contour-
data-values.yaml -n tanzu-system-ingress
```

`secret/contour-data-values` se crea en el espacio de nombres `tanzu-system-ingress`. Verifique con el siguiente comando:

```
kubectl get secrets -n tanzu-system-ingress
```

7 Implemente la aplicación del controlador de entrada de Contour.

```
kubectl apply -f contour-extension.yaml
```

Si todo es correcto, debería ver `app.kappctrl.k14s.io/contour created`.

8 Compruebe el estado de la aplicación del controlador de ingreso de Contour.

```
kubectl get app contour -n tanzu-system-ingress
```

Si es correcto, el estado cambia de `Reconciling` a `Reconcile succeeded`. Si el estado es `Reconcile failed`, consulte Solucionar problemas de implementación de entrada de Contour.

9 Vea más detalles sobre la aplicación del controlador de entrada de Contour.

```
kubectl get app contour -n tanzu-system-ingress -o yaml
```

10 Vea el servicio Envoy de tipo LoadBalancer.

```
kubectl get service envoy -n tanzu-system-ingress -o wide
```

Si es correcto, debería ver los detalles de Envoy LoadBalancer.

```
NAME    TYPE           CLUSTER-IP     EXTERNAL-IP     PORT(S)                         AGE
SELECTOR
envoy   LoadBalancer   10.79.65.110   10.178.147.73   80:30437/TCP,443:30589/TCP   2m42s
app=envoy,kapp.k14s.io/app=1629916985840017976
```

11 Compruebe el DaemonSet de Envoy.

```
kubectl get daemonsets -n tanzu-system-ingress
```

Si es correcto, debería ver el DaemonSet de Envoy de 3 pods.

```
NAME    DESIRED   CURRENT   READY   UP-TO-DATE   AVAILABLE   NODE SELECTOR   AGE
envoy   3         3         3       3            3           <none>          6m10s
```

12 Compruebe la implementación de Contour.

```
kubectl get deployments -n tanzu-system-ingress
```

Si es correcto, debería ver la implementación de Contour de 2 pods.

```
NAME      READY   UP-TO-DATE   AVAILABLE   AGE
contour   2/2     2            2           8m7s
```

13 Compruebe que el controlador de entrada de Contour esté instalado correctamente y listo para poder usarlo.

```
kubectl get pod,svc -n tanzu-system-ingress
```

El estado de los pods de Contour y Envoy debe ser `Running`, y LoadBalancer para el servicio Envoy se asigna con una `EXTERNAL-IP`.

```
NAME                            READY   STATUS    RESTARTS   AGE
pod/contour-84bb5475cf-7h4cx   1/1     Running   0          9m52s
pod/contour-84bb5475cf-v8k9r   1/1     Running   0          9m52s
pod/envoy-4828j                2/2     Running   0          9m52s
pod/envoy-c54dw                2/2     Running   0          9m52s
pod/envoy-qpjqp                2/2     Running   0          9m52s

NAME              TYPE           CLUSTER-IP     EXTERNAL-IP
PORT(S)                       AGE
service/contour   ClusterIP      10.105.6.207   <none>
8001/TCP                      9m52s
service/envoy     LoadBalancer   10.79.65.110   10.178.147.73   80:30437/
TCP,443:30589/TCP   9m52s
```

Solucionar problemas de implementación de entrada de Contour

Si se produce un error en la implementación o la reconciliación, ejecute `kubectl get pods -n tanzu-system-ingress` para ver el estado del pod. El de los pods `contour` y `envoy` debe ser `Running`. Si el estado de un pod es `ImagePullBackOff` o `ImageCrashLoopBackOff`, no se podrá extraer la imagen del contenedor. Compruebe la URL del registro en los valores de datos y los archivos YAML de extensión, y asegúrese de que sean precisos.

Compruebe los registros del contenedor, en los que `name-XXXX` es el nombre único del pod cuando ejecuta `kubectl get pods -A`:

```
kubectl logs pod/envoy-XXXXX -c envoy -n tanzu-system-ingress
```

```
 kubectl logs pod/contour-XXXXX -c contour -n tanzu-system-ingress
```

Si ve que un pod de Contour está bloqueado en un estado `ContainerCreating` sin generar ninguno de los errores de imagen anteriores y no muestra ningún progreso ("contour-xxxxx ha agotado el tiempo de espera para seguir progresando"), es probable que haya un conflicto con la dirección IP. Asegúrese de que el rango de CIDR de los nodos que especificó al configurar la red de carga de trabajo no entre en conflicto con el rango de CIDR de los pods en la especificación del clúster, el cual es de forma predeterminada `192.168.0.0/16`. Si hay un conflicto, actualice el clúster con una subred de pods diferente o cambie la red de nodos.

Actualizar la extensión Contour

Actualice la extensión de Contour que está implementada en el clúster de Tanzu Kubernetes.

1 Obtenga los valores de datos de Contour del secreto.

```
kubectl get secret contour-data-values -n tanzu-system-ingress -o 'go-
template={{ index .data "values.yaml" }}' | base64 -d > contour-data-values.yaml
```

2 Actualice los valores de datos de entrada de Contour en `ingress/contour/values.yaml`. Consulte Configurar la extensión Contour.

Por ejemplo, la siguiente configuración de Contour para vSphere utiliza un servicio de tipo LoadBalancer.

```
infrastructure_provider: "vsphere"
contour:
  image:
    repository: projects.registry.vmware.com/tkg
envoy:
  image:
    repository: projects.registry.vmware.com/tkg
    tag: v1.17.3_vmware.1
  service:
    type: "LoadBalancer"
```

Nota Se recomienda especificar la versión de imagen de Envoy `v1.17.3_vmware.1` para no utilizar la versión de imagen de Envoy `v1.16.2_vmware.1`, la cual tiene un CVE. Para obtener más información, consulte las Notas de la versión.

3 Actualice el secreto de los valores de datos de Contour.

```
kubectl create secret generic contour-data-values --from-file=values.yaml=contour-data-values.yaml -n tanzu-system-ingress -o yaml --dry-run | kubectl replace -f-
```

La extensión Contour se conciliará entonces con los nuevos valores de datos.

Nota De forma predeterminada, kapp-controller sincronizará las aplicaciones cada 5 minutos. La actualización debería tener efecto en 5 minutos o menos. Si desea que se aplique inmediatamente, cambie los valores de `syncPeriod` en `contour-extension.yaml` a un valor menor y vuelva a implementar la extensión mediante `kubectl apply -f contour-extension.yaml`.

4 Compruebe el estado de la aplicación.

```
kubectl get app contour -n tanzu-system-ingress
```

El estado debe cambiar a `Reconcile Succeeded` una vez que Contour se actualice.

5 Ver estado detallado.

```
kubectl get app contour -n tanzu-system-ingress -o yaml
```

6 Solucione los problemas en caso necesario. Consulte Solucionar problemas de implementación de entrada de Contour.

Eliminar la extensión de extensión Contour

Elimine la extensión Contour de un clúster de Tanzu Kubernetes.

Nota Complete los pasos en orden. No elimine el espacio de nombres, la cuenta de servicio ni los objetos de función antes de eliminar totalmente la aplicación del controlador de entrada de Contour. De lo contrario, podría provocar errores en el sistema.

1 Cambie el directorio a la extensión Contour.

```
cd extensions/ingress/contour/
```

2 Elimine la aplicación del controlador de entrada de Contour.

```
kubectl delete app contour -n tanzu-system-ingress
```

Resultado esperado: `app.kappctrl.k14s.io "contour" deleted`.

3 Compruebe que la aplicación del controlador de entrada de Contour se haya eliminado.

```
kubectl get app contour -n tanzu-system-ingress
```

Resultado esperado: `apps.kappctrl.k14s.io "contour" not found`.

4 Elimine el espacio de nombres `tanzu-system-ingress`, así como los objetos de función y la cuenta de servicio de la extensión Contour.

```
kubectl delete -f namespace-role.yaml
```

Actualizar la extensión Contour

Si tiene una extensión de Contour existente implementada, puede actualizarla a la versión más reciente.

1 Exporte el mapa de configuración de Contour y guárdelo como copia de seguridad.

```
kubectl get configmap contour -n tanzu-system-ingress -o 'go-template={{ index .data
"contour.yaml" }}' > contour-configmap.yaml
```

2 Elimine la implementación de Contour existente. Consulte Eliminar la extensión de extensión Contour.

3 Implemente la última extensión Contour. Consulte Implementar la extensión Contour.

Configurar la extensión Contour

Los valores de configuración del controlador de entrada de Contour se establecen en `/extensions/ingress/contour/vsphere/contour-data-values.yaml`.

Tabla 14-4. Parámetros de configuración de entrada de Contour

Parámetro	Descripción	Tipo	Predeterminado
infrastructure_provider	Proveedor de infraestructura. Valores admitidos: vsphere, aws, azure	string	Parámetro obligatorio
contour.namespace	Espacio de nombres en el que se implementará Contour	string	tanzu-system-ingress
contour.config.requestTimeout	Tiempo de espera de solicitud del cliente que se debe pasar a Envoy	time.Duration	0s Consulte Tiempo de espera de ruta para las descargas de archivo.
contour.config.server.xdsServerType	Tipo de servidor XDS que se utilizará: Valores compatibles: contour o envoy	string	Nulo
contour.config.tls.minimumProtocolVersion	Versión mínima de TLS que Contour negociará	string	1,1
contour.config.tls.fallbackCertificate.name	Nombre del secreto que contiene el certificado de reserva para las solicitudes que no coinciden con el SNI definido para un vhost	string	Nulo
contour.config.tls.fallbackCertificate.namespace	Espacio de nombres del secreto que contiene el certificado de reserva	string	Nulo
contour.config.tls.envoyClientCertificate.name	Nombre del secreto que se utilizará como certificado del cliente, clave privada para la conexión TLS al servicio back-end.	string	Nulo
contour.config.tls.envoyClientCertificate.namespace	Espacio de nombres del secreto que se utilizará como certificado del cliente, clave privada para la conexión TLS al servicio back-end.	string	Nulo
contour.config.leaderelection.configmapName	Nombre del configmap que se utilizará para contour leaderelection	string	leader-elect
contour.config.leaderelection.configmapNamespace	Espacio de nombres de contour leaderelection configmap	string	tanzu-system-ingress
contour.config.disablePermitInsecure	Deshabilita el campo ingressroute permitInsecure	booleano	false

Tabla 14-4. Parámetros de configuración de entrada de Contour (continuación)

Parámetro	Descripción	Tipo	Predeterminado
contour.config.accesslogFormat	Formato de registro de acceso	string	envoy
contour.config.jsonFields	Campos que se registrarán	array of strings	https://godoc.org/github.com/projectcontour/contour/internal/envoy#JSONFields
contour.config.useProxyProtocol	https://projectcontour.io/guides/proxy-proto/	booleano	false
contour.config.defaultHTTPVersions	Contour debería programar a Envoy para que sirva estas versiones HTTP	array of strings	"HTTP/1.1 HTTP2"
contour.config.timeouts.requestTimeout	El tiempo de espera de una solicitud completa	time.Duration	Nulo (el tiempo de espera está deshabilitado)
contour.config.timeouts.connectionIdleTimeout	El tiempo de espera antes de finalizar una conexión inactiva	time.Duration	60s
contour.config.timeouts.streamIdleTimeout	Tiempo de espera antes de finalizar una solicitud o un flujo sin actividad	time.Duration	5m
contour.config.timeouts.maxConnectionDuration	Tiempo de espera antes de finalizar una conexión, independientemente de si hay actividad o no	time.Duration	Nulo (el tiempo de espera está deshabilitado)
contour.config.timeouts.ConnectionShutdownGracePeriod	Tiempo que se debe esperar entre el envío de un GOAWAY inicial y final	time.Duration	5s
contour.config.cluster.dnsLookupFamily	dns-lookup-family que se utilizará para las solicitudes de subida a servicios de tipo externalName desde una ruta HTTPProxy	string	Nulo (valores admitidos: auto, v4, v6)
contour.config.debug	Activa la depuración de Contour	booleano	false
contour.config.ingressStatusAddress	Dirección que se establecerá en el estado de cada recurso de entrada.	string	Nulo
contour.certificate.duration	Duración del certificado de Contour	time.Duration	8760h
contour.certificate.renewBefore	Duración antes de la renovación del certificado de Contour	time.Duration	360h
contour.deployment.replicas	Número de réplicas de Contour	entero	2

Tabla 14-4. Parámetros de configuración de entrada de Contour (continuación)

Parámetro	Descripción	Tipo	Predeterminado
contour.image.repository	Ubicación del repositorio con la imagen de Contour. El valor predeterminado es el registro de VMware público. Cambie este valor si utiliza un repositorio privado (p. ej., un entorno aislado).	string	projects.registry.vmware.com/tkg
contour.image.name	Nombre de la imagen de Contour	string	contour
contour.image.tag	Etiqueta de la imagen de Contour. Es posible que este valor tenga que actualizarse si va a actualizar la versión de Contour.	string	v1.11.0_vmware.1
contour.image.pullPolicy	Directiva de extracción de imagen de Contour	string	IfNotPresent
envoy.image.repository	Ubicación del repositorio con la imagen de Envoy. El valor predeterminado es el registro de VMware público. Cambie este valor si utiliza un repositorio privado (p. ej., un entorno aislado).	string	projects.registry.vmware.com/tkg
envoy.image.name	Nombre de la imagen de Envoy	string	envoy
envoy.image.tag	Etiqueta de la imagen de Envoy. Es posible que este valor tenga que actualizarse si va a actualizar la versión de Envoy.	string	`v1.17.3_vmware.1` **Nota** No utilice la imagen de Envoy `v1.16.2_vmware.1` debido a una CVE. Para obtener más información, consulte las Notas de la versión.
envoy.image.pullPolicy	Directiva de extracción de la imagen de Envoy	string	IfNotPresent
envoy.hostPort.enable	Etiqueta para exponer los puertos de Envoy en el host	booleano	true
envoy.hostPort.http	Puerto de host HTTP de Envoy	entero	80
envoy.hostPort.https	Puerto de host HTTPS de Envoy	entero	443

Tabla 14-4. Parámetros de configuración de entrada de Contour (continuación)

Parámetro	Descripción	Tipo	Predeterminado
envoy.service.type	Tipo de servicio para exponer Envoy. Valores admitidos: ClusterIP, NodePort y LoadBalancer	string	Parámetro obligatorio para vSphere: NodePort o LoadBalancer, AWS: LoadBalancer, Azure: LoadBalancer
envoy.service.annotations	Anotaciones en el servicio Envoy	Mapa (valores de clave)	Mapa vacío
envoy.service.externalTrafficPolicy	Directiva de tráfico externo del servicio Envoy. Valores admitidos: Local, Clúster	string	Clúster
envoy.service.nodePort.http	NodePort deseado para el servicio de tipo NodePort utilizado para las solicitudes http	entero	Nulo: Kubernetes asigna un puerto de nodo dinámico
envoy.service.nodePort.https	NodePort deseado para el servicio de tipo NodePort utilizado para las solicitudes HTTPS	entero	Nulo: Kubernetes asigna un puerto de nodo dinámico
envoy.deployment.hostNetwork	Ejecuta envoy en hostNetwork	booleano	false
envoy.service.aws.LBType	Tipo AWS LB que se utilizará para exponer el servicio Envoy. Valores admitidos: clásico, nlb	string	clásico
envoy.loglevel	Nivel de registro que se utilizará para Envoy	string	info

Tiempo de espera de ruta para las descargas de archivo

El parámetro `contour.config.requestTimeout` define la duración del tiempo de espera de la ruta de Contour. El valor predeterminado es `0s`. Si utiliza Contour para la transferencia de archivos, es posible que deba ajustar este valor.

Según la documentación de Contour , un valor de tiempo de espera de `0s` indica a Contour que utilice el tiempo de espera de Envoy. Según la documentación de Envoy, Envoy tiene un tiempo de espera de 15 segundos de forma predeterminada. Además, Envoy espera que toda la operación de solicitud-respuesta se complete dentro del intervalo de tiempo de espera.

Esto significa que con la configuración predeterminada de tiempo de espera de Contour de `0s`, la transferencia de archivos debe completarse en 15 segundos. Para las transferencias de archivos grandes, es posible que este tiempo no sea suficiente. Para deshabilitar el tiempo de espera predeterminado de Envoy, establezca el valor de `contour.config.requestTimeout` en `0`.

Implementar y administrar la extensión TKG para la supervisión de Prometheus

En este tema se describe cómo implementar la extensión TKG v1.3.1 para Prometheus. Prometheus es un sistema de supervisión de sistemas y servicios. Recopila métricas de destinos configurados a intervalos determinados, evalúa las expresiones de las reglas, muestra los resultados y puede activar alertas si se observa alguna condición como verdadera. Alertmanager controla las alertas generadas por Prometheus y las enruta a sus endpoints receptores. Implemente la extensión de TKG para Prometheus para generar y ver métricas para los clústeres de Tanzu Kubernetes.

Requisitos previos de la extensión

Cumpla los siguientes requisitos antes de implementar la extensión TKG v1.3.1 para Prometheus con Alertmanager para la supervisión de clústeres.

- Aprovisionar un clúster. Consulte Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS.

  Nota Para instalar la extensión Prometheus, debe implementar un clúster que utilice el serviceDomain predeterminado (`cluster.local`).

- Conéctese al clúster. Consulte Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.
- Descargar el paquete de extensiones TKG v1.3.1 al host cliente en el que se ejecuta kubectl.
- Instalar los requisitos previos de las extensiones TKG en el clúster de Tanzu Kubernetes de destino.

Además de los requisitos generales, la supervisión de Prometheus requiere una clase de almacenamiento persistente predeterminada. Se puede crear un clúster con una clase de almacenamiento persistente predeterminada o especificar uno en el archivo de configuración de Prometheus al implementar la extensión. Consulte Revisar los requisitos previos de almacenamiento persistente para las extensiones de TKG.

Implementar la extensión Prometheus

La extensión TKG para Prometheus instala varios contenedores. Para obtener más información, consulte https://prometheus.io/.

Contenedor	Tipo de recurso	Réplicas	Descripción
`prometheus-alertmanager`	Implementación	1	Controla las alertas enviadas por las aplicaciones cliente, como el servidor Prometheus.
`prometheus-cadvisor`	DaemonSet	5	Analiza y expone datos de rendimiento y uso de recursos de los contenedores que se están ejecutando.

Contenedor	Tipo de recurso	Réplicas	Descripción
prometheus-kube-state-metrics	Implementación	1	Supervisa el estado y la capacidad del nodo, la conformidad del conjunto de réplicas, el pod, el estado del trabajo y el trabajo cron, las solicitudes de recursos y los límites.
prometheus-node-exporter	DaemonSet	5	Exportador de métricas de hardware y SO expuestas por los kernels.
prometheus-pushgateway	Implementación	1	Servicio que le permite insertar métricas de los trabajos que no se pueden extraer.
prometheus-server	Implementación	1	Proporciona funcionalidades básicas, como la extracción, el procesamiento de reglas y las alertas.

La extensión está configurada para extraer los contenedores del registro público de VMware en https://projects.registry.vmware.com/. Si utiliza un registro privado, cambie la URL del endpoint en los valores de datos y las configuraciones de extensión para que coincidan. Consulte Configurar la extensión Prometheus.

1 Asegúrese de haber completado cada uno de los requisitos previos de la extensión. Consulte Requisitos previos de la extensión.

2 Cambie el directorio a la extensión Prometheus.

```
cd /tkg-extensions-v1.3.1+vmware.1/extensions/monitoring/prometheus
```

3 Cree el espacio de nombres `tanzu-system-monitoring`, así como los objetos de función y la cuenta de servicio Prometheus.

```
kubectl apply -f namespace-role.yaml
```

4 Cree un archivo de valores de datos de Prometheus.

El archivo de valores de datos de ejemplo proporciona la configuración mínima.

```
cp prometheus-data-values.yaml.example prometheus-data-values.yaml
```

5 Configure la extensión Prometheus mediante la actualización de `prometheus-data-values.yaml`. Consulte Configurar la extensión Prometheus para ver una descripción de los campos y las opciones.

Si el clúster no se aprovisiona con una clase de almacenamiento persistente predeterminada, puede especificarla en el archivo de valores de datos. Además, asegúrese de que el espacio de nombres tenga suficiente almacenamiento para las notificaciones de volumen persistente.

```
monitoring:
  prometheus_server:
    image:
      repository: projects.registry.vmware.com/tkg/prometheus
    pvc:
      storage_class: vwt-storage-policy
```

```
      storage: "8Gi"
  alertmanager:
    image:
      repository: projects.registry.vmware.com/tkg/prometheus
    pvc:
      storage_class: vwt-storage-policy
      storage: "8Gi"
...
```

6 Cree el secreto de Prometheus con el archivo `prometheus-data-values`.

```
kubectl create secret generic prometheus-data-values --from-file=values.yaml=prometheus-data-values.yaml -n tanzu-system-monitoring
```

El secreto de `prometheus-data-values` se crea en el espacio de nombres de `tanzu-system-monitoring`. Compruébelo mediante `kubectl get secrets -n tanzu-system-monitoring`.

7 Implemente la extensión Prometheus.

```
kubectl apply -f prometheus-extension.yaml
```

Cuando finalice correctamente, se creará la aplicación Prometheus: `app.kappctrl.k14s.io/prometheus created`.

8 Compruebe el estado de la aplicación Prometheus.

```
kubectl get app prometheus -n tanzu-system-monitoring
```

El estado debe cambiar de `Reconciling` a `Reconcile succeeded`. Si el estado es `Reconcile failed`, consulte Solucionar problemas.

9 Vea información detallada sobre la aplicación Prometheus.

```
kubectl get app prometheus -n tanzu-system-monitoring -o yaml
```

10 Compruebe los DaemonSets de Prometheus.

```
kubectl get daemonsets -n tanzu-system-monitoring
```

11 Compruebe las implementaciones de Prometheus.

```
kubectl get deployments -n tanzu-system-monitoring
```

Solucionar problemas de implementación de Prometheus

Si se produce un error en la implementación o la reconciliación, ejecute `kubectl get pods -A` para ver el estado de los pods. En condiciones normales, debería ver los pods con el estado `Running`. Si el estado es `ImagePullBackOff` o `ImageCrashLoopBackOff`, quiere decir que la imagen del contenedor no se pudo extraer del registro . Compruebe la URL en los valores de datos y los archivos YAML de extensión, y asegúrese de que sean precisos.

Compruebe los registros del contenedor, en los que `name-XXXX` es el nombre único del pod cuando ejecuta `kubectl get pods -A`:

```
kubectl logs pod/prometheus-alertmanager-XXXXX -c prometheus-alertmanager -n tanzu-system-
monitoring
```

```
kubectl logs pod/prometheus-server-XXXXX -c prometheus-server -n tanzu-system-monitoring
```

Actualizar la extensión Prometheus

Actualice la configuración de una extensión de Prometheus que esté implementada en un clúster de Tanzu Kubernetes.

1 Obtenga los valores de datos de Prometheus del secreto.

```
kubectl get secret prometheus-data-values -n tanzu-system-monitoring -o 'go-
template={{ index .data "values.yaml" }}' | base64 -d > prometheus-data-values.yaml
```

2 Actualice el secreto de los valores de datos de Prometheus.

```
kubectl create secret generic prometheus-data-values --from-file=values.yaml=prometheus-
data-values.yaml -n tanzu-system-monitoring -o yaml --dry-run | kubectl replace -f-
```

La extensión Prometheus se conciliará con los valores de datos actualizados.

Nota De forma predeterminada, kapp-controller sincronizará las aplicaciones cada 5 minutos. La actualización debería tener efecto en 5 minutos o menos. Si desea que la actualización se aplique inmediatamente, cambie los valores de `syncPeriod` en `prometheus-extension.yaml` a un valor menor y aplique la extensión de Fluent Bit mediante `kubectl apply -f prometheus-extension.yaml`.

3 Compruebe el estado de la extensión.

```
kubectl get app prometheus -n tanzu-system-monitoring
```

El estado debe cambiar a `Reconcile Succeeded` una vez que Prometheus se actualice.

4 Vea el estado detallado y solucione los problemas.

```
kubectl get app prometheus -n tanzu-system-monitoring -o yaml
```

Eliminar la extensión Prometheus

Elimine la extensión Prometheus de un clúster de Tanzu Kubernetes.

Nota Complete los pasos en orden. No elimine el espacio de nombres, la cuenta de servicio ni los objetos de función antes de eliminar totalmente la aplicación de Prometheus. De lo contrario, podría provocar errores en el sistema.

Precaución Prometheus y Grafana utilizan el mismo espacio de nombres. La eliminación del espacio de nombres destruye cualquier extensión que se haya implementado allí. Si se implementa Grafana, no elimine el espacio de nombres antes de eliminar Grafana.

1 Cambie el directorio a la extensión Prometheus.

```
cd /extensions/monitoring/prometheus/
```

2 Elimine la aplicación Prometheus.

```
kubectl delete app prometheus -n tanzu-system-monitoring
```

Resultado esperado: `app.kappctrl.k14s.io "prometheus" deleted`.

3 Compruebe que el aplicación Prometheus se haya eliminado.

```
kubectl get app prometheus -n tanzu-system-monitoring
```

Resultado esperado: `apps.kappctrl.k14s.io "prometheus" not found`.

4 Elimine el espacio de nombres `tanzu-system-monitoring`, así como los objetos de función y la cuenta de servicio de Prometheus.

Advertencia No lleve a cabo este paso si Grafana está implementado.

```
kubectl delete -f namespace-role.yaml
```

5 Si desea volver a implementar Prometheus, elimine el secreto `prometheus-data-values`.

```
kubectl delete secret prometheus-data-values -n tanzu-system-monitoring
```

Resultado esperado: `secret "prometheus-data-values" deleted`.

Actualizar la extensión Prometheus

Si tiene una extensión de Prometheus existente implementada, puede actualizarla a la versión más reciente.

1 Exporte el mapa de configuración de Prometheus y guárdelo como copia de seguridad.

```
kubectl get configmap prometheus -n tanzu-system-monitoring -o 'go-template={{ index .data
"prometheus.yaml" }}' > prometheus-configmap.yaml
```

2 Elimine la implementación de Prometheus existente. Consulte Eliminar la extensión Prometheus.

3 Implemente la extensión Prometheus. Consulte Implementar la extensión Prometheus.

Configurar la extensión Prometheus

La configuración de Prometheus se establece en `/extensions/monitoring/prometheus/prometheus-data-values.yaml`.

Tabla 14-5. Parámetros de configuración de Prometheus

Parámetro	Descripción	Tipo	Predeterminado
monitoring.namespace	Espacio de nombres en el que se implementará Prometheus	string	tanzu-system-monitoring
monitoring.create_namespace	La marca indica si se debe crear el espacio de nombres especificado por monitoring.namespace	booleano	false
monitoring.prometheus_server.config.prometheus_yaml	Detalles de configuración del clúster de Kubernetes que se pasarán a Prometheus	archivo yaml	prometheus.yaml
monitoring.prometheus_server.config.alerting_rules_yaml	Reglas de alerta detalladas definidas en Prometheus	archivo yaml	alerting_rules.yaml
monitoring.prometheus_server.config.recording_rules_yaml	Reglas de registro detalladas definidas en Prometheus	archivo yaml	recording_rules.yaml
monitoring.prometheus_server.service.type	Tipo de servicio para exponer Prometheus. Valores admitidos: ClusterIP	string	ClusterIP
monitoring.prometheus_server.enable_alerts.kubernetes_api	Habilitar alertas de SLO para la API de Kubernetes en Prometheus	booleano	true
monitoring.prometheus_server.sc.aws_type	Tipo de AWS definido para storageclass en AWS	string	gp2
monitoring.prometheus_server.sc.aws_fsType	Tipo de sistema de archivos de AWS definido para storageclass en AWS	string	ext4
monitoring.prometheus_server.sc.allowVolumeExpansion	Definir si se permite la expansión de volumen para storageclass en AWS	booleano	true
monitoring.prometheus_server.pvc.annotations	Anotaciones de clase de almacenamiento	mapa	{}

Tabla 14-5. Parámetros de configuración de Prometheus (continuación)

Parámetro	Descripción	Tipo	Predeterminado
monitoring.prometheus_server.pvc.storage_class	Clase de almacenamiento que se utilizará para la notificación de volumen persistente. De forma predeterminada, es nulo y se utiliza el aprovisionador predeterminado.	string	nulo
monitoring.prometheus_server.pvc.accessMode	Defina el modo de acceso para la notificación de volumen persistente. Valores compatibles: ReadWriteOnce, ReadOnlyMany, ReadWriteMany	string	ReadWriteOnce
monitoring.prometheus_server.pvc.storage	Definir tamaño de almacenamiento para notificación de volumen persistente	string	8Gi
monitoring.prometheus_server.deployment.replicas	Cantidad de réplicas de Prometheus	entero	1
monitoring.prometheus_server.image.repository	Ubicación del repositorio con la imagen de Prometheus. El valor predeterminado es el registro de VMware público. Cambie este valor si utiliza un repositorio privado (p. ej., un entorno aislado).	string	projects.registry.vmware.com/tkg/prometheus
monitoring.prometheus_server.image.name	Nombre de la imagen de Prometheus	string	prometheus
monitoring.prometheus_server.image.tag	Etiqueta de la imagen de Prometheus. Es posible que este valor tenga que actualizarse si va a actualizar la versión.	string	v2.17.1_vmware.1
monitoring.prometheus_server.image.pullPolicy	Directiva de extracción de imágenes de Prometheus	string	IfNotPresent
monitoring.alertmanager.config.slack_demo	Configuración de notificaciones de Slack para Alertmanager	string	`slack_demo:` `  name: slack_demo` `  slack_configs:` `  -` `api_url: https://hooks.slack.com` `    channel:` `'#alertmanager-test'`

Tabla 14-5. Parámetros de configuración de Prometheus (continuación)

Parámetro	Descripción	Tipo	Predeterminado
monitoring.alertmanager.config.email_receiver	Configuración de notificaciones de correo electrónico para Alertmanager	string	`email_receiver:` `  name: email-receiver` `  email_configs:` `  - to: demo@tanzu.com` `    send_resolved: false` `    from: from-email@tanzu.com` `    smarthost: smtp.eample.com:25` `    require_tls: false`
monitoring.alertmanager.service.type	Tipo de servicio para exponer Alertmanager. Valores admitidos: ClusterIP	string	ClusterIP
monitoring.alertmanager.image.repository	Ubicación del repositorio con la imagen de Alertmanager. El valor predeterminado es el registro de VMware público. Cambie este valor si utiliza un repositorio privado (p. ej., un entorno aislado).	string	projects.registry.vmware.com/tkg/prometheus
monitoring.alertmanager.image.name	Nombre de la imagen de Alertmanager	string	alertmanager
monitoring.alertmanager.image.tag	Etiqueta de la imagen de Alertmanager. Es posible que este valor tenga que actualizarse si va a actualizar la versión.	string	v0.20.0_vmware.1
monitoring.alertmanager.image.pullPolicy	Directiva de extracción de imágenes de Alertmanager	string	IfNotPresent
monitoring.alertmanager.pvc.annotations	Anotaciones de clase de almacenamiento	mapa	{}
monitoring.alertmanager.pvc.storage_class	Clase de almacenamiento que se utilizará para la notificación de volumen persistente. De forma predeterminada, es nulo y se utiliza el aprovisionador predeterminado.	string	nulo

Tabla 14-5. Parámetros de configuración de Prometheus (continuación)

Parámetro	Descripción	Tipo	Predeterminado
monitoring.alertmanager.pvc.accessMode	Defina el modo de acceso para la notificación de volumen persistente. Valores compatibles: ReadWriteOnce, ReadOnlyMany, ReadWriteMany	string	ReadWriteOnce
monitoring.alertmanager.pvc.storage	Definir tamaño de almacenamiento para notificación de volumen persistente	string	2Gi
monitoring.alertmanager.deployment.replicas	Cantidad de réplicas de Alertmanager	entero	1
monitoring.kube_state_metrics.image.repository	Repositorio que contiene la imagen de kube-state-metircs. El valor predeterminado es el registro de VMware público. Cambie este valor si utiliza un repositorio privado (p. ej., un entorno aislado).	string	projects.registry.vmware.com/tkg/prometheus
monitoring.kube_state_metrics.image.name	Nombre contiene la imagen kube-state-metircs	string	kube-state-metrics
monitoring.kube_state_metrics.image.tag	Etiqueta de la imagen de kube-state-metircs. Es posible que este valor tenga que actualizarse si va a actualizar la versión.	string	v1.9.5_vmware.1
monitoring.kube_state_metrics.image.pullPolicy	directiva de extracción de imágenes de kube-state-metircs	string	IfNotPresent
monitoring.kube_state_metrics.deployment.replicas	Cantidad de réplicas de kube-state-metrics	entero	1
monitoring.node_exporter.image.repository	Repositorio que contiene la imagen de node-exporter. El valor predeterminado es el registro de VMware público. Cambie este valor si utiliza un repositorio privado (p. ej., un entorno aislado).	string	projects.registry.vmware.com/tkg/prometheus
monitoring.node_exporter.image.name	Nombre de la imagen de node-exporter	string	node-exporter

Tabla 14-5. Parámetros de configuración de Prometheus (continuación)

Parámetro	Descripción	Tipo	Predeterminado
monitoring.node_exporter.image.tag	Etiqueta de la imagen de node-exporter. Es posible que este valor tenga que actualizarse si va a actualizar la versión.	string	v0.18.1_vmware.1
monitoring.node_exporter.image.pullPolicy	directiva de extracción de imágenes de nodo-exporter	string	IfNotPresent
monitoring.node_exporter.hostNetwork	Si se establece en `hostNetwork: true`, el pod puede utilizar el espacio de nombres de red y los recursos de red del nodo.	booleano	false
monitoring.node_exporter.deployment.replicas	Cantidad de réplicas de node-exporter	entero	1
monitoring.pushgateway.image.repository	Repositorio que contiene la imagen de pushgateway. El valor predeterminado es el registro de VMware público. Cambie este valor si utiliza un repositorio privado (p. ej., un entorno aislado).	string	projects.registry.vmware.com/tkg/prometheus
monitoring.pushgateway.image.name	Nombre de la imagen de pushgateway	string	pushgateway
monitoring.pushgateway.image.tag	Etiqueta de la imagen de pushgateway. Es posible que este valor tenga que actualizarse si va a actualizar la versión.	string	v1.2.0_vmware.1
monitoring.pushgateway.image.pullPolicy	Directiva de extracción de imágenes de pushgateway	string	IfNotPresent
monitoring.pushgateway.deployment.replicas	Cantidad de réplicas de pushgateway	entero	1
monitoring.cadvisor.image.repository	Repositorio que contiene la imagen de cadvisor. El valor predeterminado es el registro de VMware público. Cambie este valor si utiliza un repositorio privado (p. ej., un entorno aislado).	string	projects.registry.vmware.com/tkg/prometheus
monitoring.cadvisor.image.name	Nombre de la imagen de cadvisor	string	cadvisor

Tabla 14-5. Parámetros de configuración de Prometheus (continuación)

Parámetro	Descripción	Tipo	Predeterminado
monitoring.cadvisor.image.tag	Etiqueta de la imagen de cadvisor. Es posible que este valor tenga que actualizarse si va a actualizar la versión.	string	v0.36.0_vmware.1
monitoring.cadvisor.image.pullPolicy	Directiva de extracción de imágenes de cadvisor	string	IfNotPresent
monitoring.cadvisor.deployment.replicas	Cantidad de réplicas de cadvisor	entero	1
monitoring.ingress.enabled	Habilita/deshabilita la entrada para Prometheus y Alertmanager	booleano	false Para utilizar la entrada, establezca este campo en `true` e implemente Implementar y administrar la extensión TKG para la entrada de Contour. Para acceder a Prometheus, actualice sus `/etc/hosts` locales con una entrada que asigne `prometheus.system.tanzu` a una dirección IP del nodo de trabajo.
monitoring.ingress.virtual_host_fqdn	Nombre de host para acceder a Prometheus y Alertmanager	string	prometheus.system.tanzu
monitoring.ingress.prometheus_prefix	Prefijo de ruta de acceso para Prometheus	string	/
monitoring.ingress.alertmanager_prefix	Prefijo de ruta de acceso para Alertmanager	string	/alertmanager/
monitoring.ingress.tlsCertificate.tls.crt	Certificado opcional para la entrada si desea utilizar su propio certificado TLS. De forma predeterminada, se genera un certificado autofirmado	string	Certificado generado
monitoring.ingress.tlsCertificate.tls.key	Clave privada de certificado opcional para la entrada si desea utilizar su propio certificado TLS.	string	Clave de certificado generada

Tabla 14-6. Campos configurables para Prometheus_Server Configmap

Parámetro	Descripción	Tipo	Predeterminado
evaluation_interval	Frecuencia para evaluar reglas	duration	1m
scrape_interval	Frecuencia de extracción de destinos	duration	1m
scrape_timeout	Tiempo agotado para una solicitud de extracción	duration	10s
rule_files	Los archivos de reglas especifican una lista de globs. Las reglas y las alertas se leen desde todos los archivos que coincidan	archivo yaml	
scrape_configs	Una lista de configuraciones de extracción.	lista	
job_name	El nombre del trabajo asignado a métricas recopiladas de forma predeterminada	string	
kubernetes_sd_configs	Lista de configuraciones de detección de servicios de Kubernetes.	lista	
relabel_configs	Lista de configuraciones de reetiqueta de destino.	lista	
action	Acción que se realizará en función de la coincidencia de expresión regular.	string	
regex	Expresión regular con la que coincide el valor extraído.	string	
source_labels	Las etiquetas de origen seleccionan valores de las etiquetas existentes.	string	
scheme	Configura el esquema de protocolo utilizado para las solicitudes.	string	
tls_config	Configura las opciones de TLS de la solicitud de chat.	string	
ca_file	Certificado de CA con el que se validará el certificado del servidor de API.	filename	
insecure_skip_verify	Deshabilite la validación del certificado del servidor.	booleano	

Tabla 14-6. Campos configurables para Prometheus_Server Configmap (continuación)

Parámetro	Descripción	Tipo	Predeterminado
bearer_token_file	Información opcional de autenticación del archivo de token de portador.	filename	
replacement	Valor de reemplazo contra el que se realiza un reemplazo de expresión regular si la expresión regular coincide.	string	
target_label	Etiqueta en la que el valor resultante se escribe en una acción de reemplazo.	string	

Tabla 14-7. Campos configurables para Alertmanager Configmap

Parámetro	Descripción	Tipo	Predeterminado
resolve_timeout	ResolveTimeout es el valor predeterminado que utiliza Alertmanager si la alerta no incluye EndsAt	duration	5m
smtp_smarthost	El host SMTP a través del cual se envían los correos electrónicos.	duration	1m
slack_api_url	URL de webhook de Slack.	string	global.slack_api_url
pagerduty_url	La URL de pagerduty a la que se enviarán solicitudes de API.	string	global.pagerduty_url
plantillas	Archivos desde los que se leen las definiciones de plantillas de notificación personalizadas	ruta del archivo	
group_by	agrupar las alertas por etiqueta	string	
group_interval	Establezca el tiempo de espera antes de enviar una notificación sobre nuevas alertas que se agregan a un grupo	duration	5m
group_wait	Tiempo que se debe esperar inicialmente para enviar una notificación para un grupo de alertas	duration	30s

Tabla 14-7. Campos configurables para Alertmanager Configmap (continuación)

Parámetro	Descripción	Tipo	Predeterminado
repeat_interval	Tiempo de espera antes de volver a enviar una notificación si ya se ha enviado correctamente para una alerta	duration	4h
receivers	Una lista de receptores de notificaciones.	lista	
severity	Gravedad del incidente.	string	
channel	El canal o el usuario al que se enviarán notificaciones.	string	
html	El cuerpo HTML de la notificación por correo electrónico.	string	
text	El cuerpo de texto de la notificación por correo electrónico.	string	
send_resolved	Indica si se informa sobre las alertas resueltas.	filename	
email_configs	Configuraciones para la integración del correo electrónico	booleano	

Las anotaciones en los pods permiten un control preciso del proceso de extracción. Estas anotaciones deben formar parte de los metadatos del pod. No tendrán efecto si se establecen en otros objetos, como Services o DaemonSets.

Tabla 14-8. Anotaciones del pod de Prometheus

Anotación del pod	Descripción
`prometheus.io/scrape`	La configuración predeterminada extraerá en todos los pods y, si se establece en false, esta anotación excluirá el pod del proceso de extracción.
`prometheus.io/path`	Si la ruta de las métricas no es /metrics, defínala con esta anotación.
`prometheus.io/port`	Realice la extracción del pod en el puerto indicado en lugar de en los puertos declarados del pod (el valor predeterminado es un destino sin puertos si no se declara ninguno).

El siguiente manifiesto de DaemonSet indicará a Prometheus que realiza la extracción de todos sus pods en el puerto 9102.

```
apiVersion: apps/v1beta2 # for versions before 1.8.0 use extensions/v1beta1
kind: DaemonSet
metadata:
  name: fluentd-elasticsearch
  namespace: weave
  labels:
    app: fluentd-logging
spec:
  selector:
    matchLabels:
      name: fluentd-elasticsearch
  template:
    metadata:
      labels:
        name: fluentd-elasticsearch
      annotations:
        prometheus.io/scrape: 'true'
        prometheus.io/port: '9102'
    spec:
      containers:
      - name: fluentd-elasticsearch
        image: gcr.io/google-containers/fluentd-elasticsearch:1.20
```

Implementar y administrar la extensión TKG para la supervisión de Grafana

En este tema se describe cómo implementar y administrar la extensión TKG v1.3.1 para Grafana. Grafana permite consultar, visualizar, alertar y explorar métricas independientemente de dónde se almacenen. Grafana proporciona herramientas para formar gráficos y visualizaciones a partir de los datos de la aplicación. Implemente la extensión de TKG para Grafana para generar y ver métricas para los clústeres de Tanzu Kubernetes.

Requisitos previos de la extensión Grafana

Cumpla con los siguientes requisitos previos para implementar la extensión.

- Aprovisionar un clúster. Consulte Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS.

  Nota Debe implementar un clúster que utilice el serviceDomain predeterminado (`cluster.local`).

- Conéctese al clúster. Consulte Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.
- Descargar el paquete de extensiones TKG v1.3.1 al host cliente en el que se ejecutan los comandos kubectl.

- Instalar los requisitos previos de las extensiones TKG en el clúster de destino.

Requisitos adicionales de la extensión Grafana

La extensión TKG v1.3.1 para supervisión de Grafana tiene requisitos adicionales que se deben tener en cuenta antes y después de la instalación.

- La extensión de supervisión de Grafana requiere una clase de almacenamiento persistente predeterminada. Se puede crear un clúster con una clase de almacenamiento persistente predeterminada o especificar uno en el archivo de configuración de Grafana al implementar la extensión. Consulte Revisar los requisitos previos de almacenamiento persistente para las extensiones de TKG.
- Una vez implementada la extensión Grafana, puede acceder al panel de control de Grafana a través de HTTP/S mediante la dirección IP expuesta por uno de los siguientes tipos de servicio de Kubernetes: ClusterIP (predeterminado), NodePort o LoadBalancer. Para acceder al panel de control de Grafana desde fuera del clúster, implemente la extensión Contour antes de implementar Grafana. Para implementar la extensión Contour, consulte Implementar y administrar la extensión TKG para la supervisión de Grafana.

  Grafana admite los siguientes tipos de servicio de Kubernetes:

Tipo de servicio	Descripción	Accesibilidad
`ClusterIP`	Expone el servicio en una IP interna del clúster.	Solo se puede acceder al servicio desde el clúster.
`NodePort`	Expone el servicio en la IP de cada nodo en un puerto estático.	Se puede acceder al servicio desde fuera del clúster.
`LoadBalancer`	Expone el servicio de forma externa mediante un equilibrador de carga.	Se puede acceder al servicio desde fuera del clúster.

  `ClusterIP` es el predeterminado, pero solo se puede acceder a él desde dentro del clúster. Si utiliza redes de NSX-T para el clúster supervisor, cree un servicio Envoy de Contour de tipo LoadBalancer. Si utiliza redes de vSphere vDS para el clúster supervisor, cree un servicio Envoy de Contour de tipo LoadBalancer o NodePort, en función de sus necesidades.

Implementar la extensión Grafana para la visualización y el análisis

La extensión TKG para Grafana implementa un único contenedor. Para obtener más información, consulte https://grafana.com/.

Contenedor	Tipo de recurso	Réplicas	Descripción
Grafana	Implementación	2	Visualización de datos

La extensión está configurada para extraer los contenedores del registro público de VMware en https://projects.registry.vmware.com/. Si utiliza un registro privado, cambie la URL del endpoint en los valores de datos y las configuraciones de extensión para que coincidan. Consulte Configurar la extensión Grafana.

1 Asegúrese de haber completado cada uno de los requisitos previos de la extensión Grafana. Consulte Requisitos previos de la extensión Grafana.

2 Cambie el directorio a la extensión Grafana.

```
cd /tkg-extensions-v1.3.1+vmware.1/extensions/monitoring/grafana
```

3 Cree el espacio de nombres `tanzu-system-monitoring` y los objetos de función y la cuenta de servicio de Grafana.

```
kubectl apply -f namespace-role.yaml
```

4 Cree un archivo de valores de datos de Grafana.

El archivo de valores de datos de ejemplo proporciona la configuración mínima que se pide.

```
cp grafana-data-values.yaml.example grafana-data-values.yaml
```

5 Configure la extensión Grafana mediante la actualización de `grafana-data-values.yaml`.

Personalice la configuración según sea necesario. Consulte Configurar la extensión Grafana.

La `admin_password` debe estar codificada en base64, aunque la implementación de la extensión no se bloqueará si no es así. En el siguiente ejemplo, la contraseña "admin" está codificada en base64. Codifique su propia contraseña de Grafana aquí: https://www.base64encode.org/.

Si el clúster no está aprovisionado con una clase de almacenamiento predeterminada, puede especificarlo en el archivo de valores de datos. Además, asegúrese de que el espacio de nombres tenga suficiente almacenamiento para las notificaciones de volumen persistente.

```
monitoring:
  grafana:
    image:
      repository: "projects.registry.vmware.com/tkg/grafana"
    pvc:
      storage_class: vwt-storage-policy
      storage: "8Gi"
    secret:
      admin_password: "YWRtaW4="
  grafana_init_container:
    image:
      repository: "projects.registry.vmware.com/tkg/grafana"
  grafana_sc_dashboard:
    image:
      repository: "projects.registry.vmware.com/tkg/grafana"
```

Si implementó Contour con un servicio Envoy de tipo LoadBalancer o NodePort, especifique eso en el archivo de configuración como se muestra. Consulte Configurar la extensión Grafana para obtener más información.

```
monitoring:
  grafana:
    service:
      type: LoadBalancer OR NodePort
```

De forma predeterminada, la extensión Grafana crea el nombre de dominio completo (Fully Qualified Domain Name, FQDN) `grafana.system.tanzu` para acceder al panel de control de Grafana. Para personalizar este FQDN, especifique el nombre de host que desee en el archivo de configuración en `monitoring.grafana.ingress.virtual_host_fqdn`. Consulte Configurar la extensión Grafana para obtener más información.

6 Cree el secreto de Grafana con el archivo `grafana-data-values`.

```
kubectl create secret generic grafana-data-values --from-file=values.yaml=grafana-data-
values.yaml -n tanzu-system-monitoring
```

El secreto de `grafana-data-values` se crea en el espacio de nombres de `tanzu-system-monitoring`. Compruébelo mediante `kubectl get secrets -n tanzu-system-monitoring`.

7 Implemente la extensión Grafana.

```
kubectl apply -f grafana-extension.yaml
```

Cuando finalice correctamente, se creará la aplicación Grafana: `app.kappctrl.k14s.io/grafana created`.

8 Compruebe el estado de la aplicación Grafana.

```
kubectl get app grafana -n tanzu-system-monitoring
```

El estado debe cambiar de `Reconciling` a `Reconcile succeeded`. Si el estado es `Reconcile failed`, consulte Solucionar problemas.

9 Vea el estado detallado de la aplicación Grafana.

```
kubectl get app grafana -n tanzu-system-monitoring -o yaml
```

10 Compruebe la implementación de Grafana.

```
kubectl get deployments -n tanzu-system-monitoring
```

Acceder al panel de control de Grafana mediante un servicio Envoy de Contour de tipo LoadBalancer

Si se implementa el servicio Contour Envoy de tipo LoadBalancer como requisito previo y lo especificó en el archivo de configuración de Grafana, obtenga la dirección IP externa del equilibrador de carga y cree registros de DNS para el FQDN de Grafana.

1 Obtenga la dirección `External-IP` para el servicio Envoy de tipo LoadBalancer.

   ```
   kubectl get service envoy -n tanzu-system-ingress
   ```

   Debería ver la dirección `External-IP` que se devuelve, por ejemplo:

   ```
   NAME    TYPE          CLUSTER-IP     EXTERNAL-IP     PORT(S)                      AGE
   envoy   LoadBalancer  10.99.25.220   10.195.141.17   80:30437/TCP,443:30589/TCP   3h27m
   ```

   Si lo prefiere, puede obtener la dirección `External-IP` mediante el siguiente comando.

   ```
   kubectl get svc envoy -n tanzu-system-ingress -o
   jsonpath='{.status.loadBalancer.ingress[0]}'
   ```

2 Para comprobar la instalación de la extensión Grafana, actualice el archivo `/etc/hosts` local con el FQDN de Grafana asignado a la dirección `External-IP` del equilibrador de carga, como por ejemplo:

   ```
   127.0.0.1 localhost
   127.0.1.1 ubuntu
   # TKG Grafana Extension with Envoy Load Balancer
   10.195.141.17 grafana.system.tanzu
   ```

3 Para acceder al panel de control de Grafana, desplácese hasta https://grafana.system.tanzu.

   Dado que el sitio utiliza certificados autofirmados, es posible que tenga que pasar por una advertencia de seguridad específica del navegador antes de poder acceder al panel de control.

4 Para el acceso de producción, cree dos registros CNAME en un servidor DNS que asignen la dirección `External-IP` del equilibrador de carga del servicio Envoy al panel de control de Grafana.

Acceder al panel de control de Grafana mediante un servicio Contour Envoy de tipo NodePort

Si se implementa el servicio Contour Envoy de tipo NodePort como requisito previo y lo especificó en el archivo de configuración de Grafana, obtenga la dirección IP de la máquina virtual de un nodo de trabajo y cree registros de DNS para el FQDN de Grafana.

1 Cambie el contexto a la instancia de espacio de nombres de vSphere en la que se aprovisiona el clúster.

```
kubectl config use-context VSPHERE-NAMESPACE
```

2 Enumere los nodos del clúster.

```
kubectl get virtualmachines
```

Debería ver los nodos del clúster; por ejemplo:

```
NAME                                              POWERSTATE   AGE
tkgs-cluster-X-control-plane-6dgln                poweredOn    6h7m
tkgs-cluster-X-control-plane-j6hq6                poweredOn    6h10m
tkgs-cluster-X-control-plane-xc25f                poweredOn    6h14m
tkgs-cluster-X-workers-9twdr-59bc54dc97-kt4cm     poweredOn    6h12m
tkgs-cluster-X-workers-9twdr-59bc54dc97-pjptr     poweredOn    6h12m
tkgs-cluster-X-workers-9twdr-59bc54dc97-t45mn     poweredOn    6h12m
```

3 Seleccione uno de los nodos de trabajo y describa el nodo mediante el siguiente comando.

```
kubectl describe virtualmachines tkgs-cluster-X-workers-9twdr-59bc54dc97-kt4cm
```

4 Busque la dirección IP de la máquina virtual; por ejemplo, `Vm Ip: 10.115.22.43`.

5 Para comprobar la instalación de la extensión Grafana, actualice el archivo `/etc/hosts` local con el FQDN de Grafana asignado a una dirección IP de nodo de trabajo, como por ejemplo:

```
127.0.0.1 localhost
127.0.1.1 ubuntu
# TKGS Grafana with Envoy NodePort
10.115.22.43 grafana.system.tanzu
```

6 Para acceder al panel de control de Grafana, desplácese hasta https://grafana.system.tanzu.

Dado que el sitio utiliza certificados autofirmados, es posible que tenga que pasar por una advertencia de seguridad específica del navegador antes de poder acceder al panel de control.

Solucionar problemas originados en la implementación de Grafana

Si se produce un error en la implementación o la reconciliación, ejecute `kubectl get pods -A` para ver el estado del pod. El de los pods `contour` y `envoy` debe ser `Running`. Si el estado de un pod es `ImagePullBackOff` o `ImageCrashLoopBackOff`, no se podrá extraer la imagen del contenedor. Compruebe la URL del registro en los valores de datos y los archivos YAML de extensión, y asegúrese de que sean precisos.

Compruebe los registros del contenedor, en los que `name-XXXX` es el nombre único del pod cuando ejecuta `kubectl get pods -A`:

```
kubectl logs pod/grafana-XXXX -c grafana -n tanzu-system-monitoring
```

Actualizar la extensión Grafana

Actualice la extensión Grafana que está implementada en el clúster de Tanzu Kubernetes.

1 Obtenga los valores de datos actuales de Grafana del secreto de `grafana-data-values`.

```
kubectl get secret grafana-data-values -n tanzu-system-monitoring -o 'go-
template={{ index .data "values.yaml" }}' | base64 -d > grafana-data-values.yaml
```

2 Actualice los valores de datos de Grafana en `grafana-data-values.yaml`. Consulte Configurar la extensión Grafana.

3 Actualice el secreto de los valores de datos de Grafana.

```
kubectl create secret generic grafana-data-values --from-file=values.yaml=grafana-data-
values.yaml -n tanzu-system-monitoring -o yaml --dry-run | kubectl replace -f-
```

La extensión Grafana se concilia con los valores de datos actualizados.

Nota De forma predeterminada, kapp-controller sincronizará las aplicaciones cada 5 minutos. La actualización debería tener efecto en 5 minutos o menos. Si desea que la actualización se aplique inmediatamente, cambie los valores de `syncPeriod` en `grafana-extension.yaml` a un valor menor y aplique la extensión de Grafana mediante `kubectl apply -f grafana-extension.yaml`.

4 Compruebe el estado de la extensión.

```
kubectl get app grafana -n tanzu-system-monitoring
```

El estado debe cambiar a `Reconcile Succeeded` una vez que Grafana se actualice.

5 Vea el estado detallado y solucione los problemas si es necesario.

```
kubectl get app grafana -n tanzu-system-monitoring -o yaml
```

Eliminar la extensión Grafana

Elimine la extensión Grafana de un clúster de Tanzu Kubernetes.

Nota Complete los pasos en orden. No elimine el espacio de nombres, la cuenta de servicio ni los objetos de función antes de eliminar totalmente la aplicación de Grafana. De lo contrario, podría provocar errores en el sistema.

Nota Las extensiones Prometheus y Grafana se implementan en el mismo espacio de nombres: `tanzu-system-monitoring`. Si implementó ambas extensiones en el mismo clúster, elimine cada extensión antes de eliminar el espacio de nombres.

1 Cambie el directorio a la extensión Grafana.

```
cd /tkg-extensions-v1.3.1+vmware.1/extensions/monitoring/grafana
```

2 Elimine la aplicación Grafana.

```
kubectl delete app grafana -n tanzu-system-monitoring
```

Resultado esperado: `app.kappctrl.k14s.io "grafana" deleted`.

3 Compruebe que la aplicación Grafana se haya eliminado.

```
kubectl get app grafana -n tanzu-system-monintoring
```

Resultado esperado: `apps.kappctrl.k14s.io "grafana" not found`.

4 Elimine el espacio de nombres `tanzu-system-monitoring`, así como los objetos de función y la cuenta de servicio de Grafana.

Advertencia No lleve a cabo este paso si Prometheus está implementado.

```
kubectl delete -f namespace-role.yaml
```

5 Si desea volver a implementar Grafana, elimine el secreto `grafana-data-values`.

```
kubectl delete secret grafana-data-values -n tanzu-system-monitoring
```

Resultado esperado: `secret "grafana-data-values" deleted`.

Actualizar la extensión Grafana

Si tiene una extensión de Grafana existente implementada, puede actualizarla a la versión más reciente.

1 Exporte el mapa de configuración de Grafana y guárdelo como copia de seguridad.

```
kubectl get configmap grafana -n tanzu-system-monitoring -o 'go-template={{ index .data
"grafana.yaml" }}' > grafana-configmap.yaml
```

2 Elimine la extensión Grafana existente. Consulte Eliminar la extensión Grafana.

3 Implemente la extensión Grafana. Consulte Implementar la extensión Grafana para la visualización y el análisis.

Configurar la extensión Grafana

La configuración de Grafana se establece en `/tkg-extensions-v1.3.1+vmware.1/extensions/monitoring/grafana/grafana-data-values.yaml`.

Tabla 14-9. Parámetros de configuración de Grafana

Parámetro	Descripción	Tipo	Predeterminado
monitoring.namespace	Espacio de nombres en el que se implementará Prometheus	string	tanzu-system-monitoring
monitoring.create_namespace	La marca indica si se debe crear el espacio de nombres especificado por monitoring.namespace	booleano	false
monitoring.grafana.cluster_role.apiGroups	grupo de API definido para grafana clusterrole	lista	[""]
monitoring.grafana.cluster_role.resources	recursos definidos para grafana clusterrole	lista	["configmaps", "secrets"]
monitoring.grafana.cluster_role.verbs	permiso de acceso definido para clusterrole	lista	["get", "watch", "list"]
monitoring.grafana.config.grafana_ini	Detalles del archivo de configuración de Grafana	archivo de configuración	grafana.ini En este archivo, la URL `grafana_net` se utiliza para integrar con Grafana. Por ejemplo, para importar el panel de control directamente desde Grafana.com.
monitoring.grafana.config.datasource.type	Tipo de origen de datos de Grafana	string	prometheus
monitoring.grafana.config.datasource.access	modo de acceso. proxy o directo (servidor o navegador en la interfaz de usuario)	string	proxy
monitoring.grafana.config.datasource.isDefault	marcar como origen de datos predeterminado de Grafana	booleano	true
monitoring.grafana.config.provider_yaml	Archivo de configuración para definir el proveedor del panel de control de grafana	archivo yaml	provider.yaml

Tabla 14-9. Parámetros de configuración de Grafana (continuación)

Parámetro	Descripción	Tipo	Predeterminado
monitoring.grafana.service.type	Tipo de servicio para exponer Grafana. Valores admitidos: ClusterIP, NodePort y LoadBalancer	string	vSphere: NodePort, aws/azure: LoadBalancer
monitoring.grafana.pvc.storage_class	Defina el modo de acceso para la notificación de volumen persistente. Valores compatibles: ReadWriteOnce, ReadOnlyMany, ReadWriteMany	string	ReadWriteOnce
monitoring.grafana.pvc.storage	Definir tamaño de almacenamiento para notificación de volumen persistente	string	2Gi
monitoring.grafana.deployment.replicas	Cantidad de réplicas de Grafana	entero	1
monitoring.grafana.image.repository	Ubicación del repositorio con la imagen de Grafana. El valor predeterminado es el registro de VMware público. Cambie este valor si utiliza un repositorio privado (p. ej., un entorno aislado).	string	projects.registry.vmware.com/tkg/grafana
monitoring.grafana.image.name	Nombre de la imagen de Grafana	string	grafana
monitoring.grafana.image.tag	Etiqueta de la imagen de Grafana. Es posible que este valor tenga que actualizarse si va a actualizar la versión.	string	v7.3.5_vmware.1
monitoring.grafana.image.pullPolicy	Directiva de extracción de imágenes de Grafana	string	IfNotPresent
monitoring.grafana.secret.type	Tipo de secreto definido para el panel de control de Grafana	string	Opaco
monitoring.grafana.secret.admin_user	nombre de usuario para acceder al panel de control de Grafana	string	YWRtaW4= El valor tiene codificación base64; para descodificar: `echo "xxxxxx" | base64 --decode`
monitoring.grafana.secret.admin_password	contraseña para acceder al panel de control de Grafana	string	nulo

Tabla 14-9. Parámetros de configuración de Grafana (continuación)

Parámetro	Descripción	Tipo	Predeterminado
monitoring.grafana.secret.ldap_toml	Si utiliza la autenticación LDAP, la ruta del archivo de configuración LDAP	string	""
monitoring.grafana_init_container.image.repository	Repositorio que contiene una imagen de contenedor de init de Grafana. El valor predeterminado es el registro de VMware público. Cambie este valor si utiliza un repositorio privado (p. ej., un entorno aislado).	string	projects.registry.vmware.com/tkg/grafana
monitoring.grafana_init_container.image.name	Nombre de la imagen de contenedor de init de Grafana	string	k8s-sidecar
monitoring.grafana_init_container.image.tag	Etiqueta de la imagen de contenedor de init de Grafana. Es posible que este valor tenga que actualizarse si va a actualizar la versión.	string	0.1.99
monitoring.grafana_init_container.image.pullPolicy	directiva de extracción de imágenes de contenedor de init de Grafana	string	IfNotPresent
monitoring.grafana_sc_dashboard.image.repository	Repositorio que contiene la imagen del panel de control de Grafana. El valor predeterminado es el registro de VMware público. Cambie este valor si utiliza un repositorio privado (p. ej., un entorno aislado).	string	projects.registry.vmware.com/tkg/grafana
monitoring.grafana_sc_dashboard.image.name	Nombre de la imagen del panel de control de Grafana	string	k8s-sidecar
monitoring.grafana_sc_dashboard.image.tag	Etiqueta de la imagen del panel de control de Grafana. Es posible que este valor tenga que actualizarse si va a actualizar la versión.	string	0.1.99
monitoring.grafana_sc_dashboard.image.pullPolicy	directiva de extracción de imagen del panel de control de Grafana	string	IfNotPresent
monitoring.grafana.ingress.enabled	Habilita/inhabilita la entrada para Grafana	booleano	true

Tabla 14-9. Parámetros de configuración de Grafana (continuación)

Parámetro	Descripción	Tipo	Predeterminado
monitoring.grafana.ingress.virtual_host_fqdn	Nombre de host para acceder a Grafana	string	grafana.system.tanzu
monitoring.grafana.ingress.prefix	Prefijo de la ruta de acceso para Grafana	string	/
monitoring.grafana.ingress.tlsCertificate.tls.crt	Certificado opcional para la entrada si desea utilizar su propio certificado TLS. De forma predeterminada, se genera un certificado autofirmado	string	Certificado generado
monitoring.grafana.ingress.tlsCertificate.tls.key	Clave privada de certificado opcional para la entrada si desea utilizar su propio certificado TLS.	string	Clave de certificado generada

Implementar y administrar la extensión TKG para el registro de Harbor

Harbor es un registro de contenedor de código abierto. La extensión TKG se puede implementar para el registro de Harbor como un almacén de registro privado para las imágenes de contenedor que desea implementar en los clústeres de Tanzu Kubernetes.

Dependencias de las versiones de extensión Harbor

Cumpla los siguientes requisitos mínimos de la versión para instalar la extensión TKG del registro Harbor en un clúster de Tanzu Kubernetes aprovisionado por servicio Tanzu Kubernetes Grid.

Componente	Versión mínima
vCenter Server	7.0.2.00400
espacio de nombres de vSphere	0.0.10-18245956
clúster supervisor	v1.20.2+vmware.1-vsc0.0.10-18245956
versión de Tanzu Kubernetes	v1.20.7+vmware.1-tkg.1.7fb9067

Requisitos previos de la extensión Harbor

Cumpla los siguientes requisitos previos antes de implementar la extensión TKG v1.3.1 para el registro de Harbor.

- Aprovisionar un clúster. Consulte Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS.
- Conéctese al clúster. Consulte Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.
- Descargar el paquete de extensiones TKG v1.3.1 al host cliente en el que se ejecutan los comandos kubectl.

- Instalar los requisitos previos de las extensiones TKG en el clúster de destino.

Requisitos adicionales de la extensión Harbor

La extensión TKG v1.3.1 para el registro de Harbor tiene requisitos adicionales que se deben tener en cuenta antes y después de la instalación.

- La extensión de Harbor requiere de una clase de almacenamiento de PVC predeterminada. Consulte Revisar los requisitos previos de almacenamiento persistente para las extensiones de TKG.
- La extensión Harbor requiere la entrada de HTTP/S. Específicamente, los servicios Harbor se exponen a través de un servicio Envoy en la extensión Contour. Como requisito previo, implemente la extensión Contour. Consulte Implementar y administrar la extensión TKG para la entrada de Contour.
  - Si utiliza redes de NSX-T para el clúster supervisor, cree un servicio Envoy de tipo LoadBalancer.
  - Si utiliza redes de vSphere vDS para el clúster supervisor, cree un servicio Envoy de tipo LoadBalancer o de tipo NodePort, según cuál sea el entorno y los requisitos.
- La extensión Harbor requiere de DNS. Después de instalar la extensión Harbor, debe configurar el DNS.
  - Para fines de realización de pruebas y verificación, agregue los FQDN de Harbor y Notary al archivo local `/etc/hosts`. Las instrucciones que aparecen a continuación describen cómo hacerlo.
  - En la fase de producción, Harbor requiere una zona DNS en un servidor DNS local, como BIND, o en una nube pública, como AWS Route53, Azure DNS o Google CloudDNS. Una vez que haya configurado DNS, instale la extensión DNS externo si desea registrar automáticamente los FQDN de Harbor con un servidor DNS. Consulte Implementar y administrar la extensión TKG para la detección de servicios de DNS externos.

Implementar la extensión Harbor

La extensión TKG del registro de Harbor instala varios contenedores en el clúster. Para obtener más información, consulte https://goharbor.io/.

Contenedor	Tipo de recurso	Réplicas	Descripción
`harbor-core`	Implementación	1	Servidor de administración y configuración para Envoy
`harbor-database`	Pod	1	Base de datos de Postgres
`harbor-jobservice`	Implementación	1	Servicio de trabajo de Harbor
`harbor-notary-server`	Implementación	1	Servicio notarial de Harbor
`harbor-notary-signer`	Implementación	1	Notary de Harbor
`harbor-portal`	Implementación	1	Interfaz web de Harbor
`harbor-redis`	Pod	1	Instancia de Redis de Harbor

Contenedor	Tipo de recurso	Réplicas	Descripción
`harbor-registry`	Implementación	2	Instancia de registro de contenedor de Harbor
`harbor-trivy`	Pod	1	Escáner de vulnerabilidad de imagen de Harbor

Para instalar el registro de Harbor con la extensión TKG, complete los siguientes pasos.

1 Asegúrese de haber completado cada uno de los requisitos previos de la extensión. Consulte Requisitos previos de la extensión Harbor y Requisitos adicionales de la extensión Harbor.

2 Cambie el directorio a la extensión Harbor.

```
cd /tkg-extensions-v1.3.1+vmware.1/extensions/registry/harbor
```

3 Cree el espacio de nombres `tanzu-system-registry`, así como las funciones y la cuenta de servicio de Harbor.

```
kubectl apply -f namespace-role.yaml
```

4 Cree un archivo de valores de datos de Harbor.

```
cp harbor-data-values.yaml.example harbor-data-values.yaml
```

5 Especifique las contraseñas y los secretos obligatorios en `harbor-data-values.yaml`.

El registro de Harbor requiere varias contraseñas y secretos enumerados y descritos en la tabla.

Contraseña o secreto	Descripción
`harborAdminPassword`	La contraseña inicial del administrador de Harbor.
`secretKey`	La clave secreta utilizada para el cifrado. Debe ser una cadena de 16 caracteres.
`database.password`	La contraseña inicial de la base de datos Postgres.
`core.secret`	El secreto se utiliza cuando el servidor principal se comunica con otro componente.
`core.xsrfKey`	La clave XSRF. Debe ser una cadena de 32 caracteres.
`jobservice.secret`	El secreto se utiliza cuando el servicio de trabajo se comunica con otro componente.
`registry.secret`	El secreto se utiliza para proteger el estado de carga del back-end de almacenamiento del cliente y del registro.

Para generar automáticamente contraseñas y secretos aleatorios y rellenar el archivo `harbor-data-values.yaml`, ejecute el siguiente comando:

```
bash generate-passwords.sh harbor-data-values.yaml
```

Una vez se realice correctamente, debería ver el siguiente mensaje:

```
Successfully generated random passwords and secrets in harbor-data-values.yaml
```

Abra el archivo harbor-data-values.yaml y compruebe las contraseñas y los secretos obligatorios.

6 En caso necesario, especifique otros valores de configuración de Harbor en harbor-data-values.yaml. Los valores más actualizados pueden incluir lo siguiente:

Campo de configuración	Descripción
hostname	El nombre de host predeterminado de Harbor es core.harbor.domain. Si es necesario, cambie este valor para que coincida con sus requisitos.
port.https	El valor predeterminado es 443. Si utiliza redes de NSX-T para el clúster supervisor y, por lo tanto, un servicio de entrada Envoy de tipo LoadBalancer, deje esta opción como el valor 443 predeterminado. Si utiliza redes de vDS para el clúster supervisor y, por lo tanto, un servicio de entrada Envoy de tipo NodePort, establezca este valor de modo que coincida con el puerto del nodo Envoy.
clair.enabled	El escáner de imágenes Clair está en desuso en favor de Trivy. Ambos están habilitados en el archivo de configuración. Para deshabilitar Clair, establezca su valor en false.
persistence.persistentVolumeClaim.<component>.accessMode	Existen varias instancias de esta configuración. El valor predeterminado es ReadWriteOnce. ReadWriteMany está programado para ser compatible en una próxima versión.
imageChartStorage.type	El valor predeterminado es filesystem. Cámbielo si es necesario y configure el almacenamiento que está utilizando.
proxy	Si lo desea, configure un proxy para Harbor. En tal caso, se necesitarán los valores noProxy predeterminados.

7 Cree un secreto con los valores de datos.

```
kubectl create secret generic harbor-data-values --from-file=values.yaml=harbor-data-
values.yaml -n tanzu-system-registry
```

secret/harbor-data-values se crea en el espacio de nombres tanzu-system-registry. Compruebe que esto es así ejecutando el siguiente comando:

```
kubectl get secrets -n tanzu-system-registry
```

8 Implemente la extensión Harbor.

```
kubectl apply -f harbor-extension.yaml
```

Si todo es correcto, debería ver `app.kappctrl.k14s.io/harbor created`.

9 Compruebe el estado de la aplicación Harbor.

```
kubectl get app harbor -n tanzu-system-registry
```

Si es correcto, el estado cambia de `Reconciling` a `Reconcile succeeded`.

```
NAME     DESCRIPTION   SINCE-DEPLOY   AGE
harbor   Reconciling   96s            98s
```

```
NAME     DESCRIPTION           SINCE-DEPLOY   AGE
harbor   Reconcile succeeded   39s            2m29s
```

Si el estado es `Reconcile failed`, consulte Solucionar problemas generados en la implementación del registro de Harbor.

10 Vea los detalles de la extensión Harbor.

```
kubectl get app harbor -n tanzu-system-registry -o yaml
```

11 Vea el estado de los objetos de implementación de Harbor.

```
kubectl get deployments -n tanzu-system-registry
```

Si es correcto, debería ver las siguientes implementaciones:

```
NAME                   READY   UP-TO-DATE   AVAILABLE   AGE
harbor-core            1/1     1            1           5m16s
harbor-jobservice      1/1     1            1           5m16s
harbor-notary-server   1/1     1            1           5m16s
harbor-notary-signer   1/1     1            1           5m16s
harbor-portal          1/1     1            1           5m16s
harbor-registry        1/1     1            1           5m16s
```

12 Vea el estado de los pods de Harbor:

```
kubectl get pods -n tanzu-system-registry
```

```
NAME                                    READY   STATUS    RESTARTS   AGE
harbor-core-9cbf4b79d-gxvgx             1/1     Running   0          7m11s
harbor-database-0                       1/1     Running   0          7m11s
harbor-jobservice-6b656ccb95-lm47d      1/1     Running   0          7m11s
harbor-notary-server-8494c684db-gm7jf   1/1     Running   0          7m11s
```

```
harbor-notary-signer-6f96b549d4-dzcnm   1/1     Running   0          7m11s
harbor-portal-5b8f4ddbd-qdnp2           1/1     Running   0          7m11s
harbor-redis-0                          1/1     Running   0          7m11s
harbor-registry-688894c58d-72txm        2/2     Running   0          7m11s
harbor-trivy-0                          1/1     Running   0          7m11s
```

13 Solucione los problemas de la instalación de Harbor, si es necesario. Consulte Solucionar problemas generados en la implementación del registro de Harbor.

Configurar DNS para Harbor mediante un servicio Envoy de tipo LoadBalancer (redes de NSX-T)

Si el servicio Envoy de requisitos previos se expone a través de LoadBalancer, obtenga la dirección IP externa del equilibrador de carga y cree registros de DNS para los FQDN de Harbor.

1 Obtenga la dirección `External-IP` para el servicio Envoy de tipo LoadBalancer.

```
kubectl get service envoy -n tanzu-system-ingress
```

Debería ver la dirección `External-IP` que se devuelve, por ejemplo:

```
NAME    TYPE           CLUSTER-IP     EXTERNAL-IP     PORT(S)                       AGE
envoy   LoadBalancer   10.99.25.220   10.195.141.17   80:30437/TCP,443:30589/TCP    3h27m
```

Si lo prefiere, puede obtener la dirección `External-IP` mediante el siguiente comando.

```
kubectl get svc envoy -n tanzu-system-ingress -o
jsonpath='{.status.loadBalancer.ingress[0]}'
```

2 Para comprobar la instalación de la extensión Harbor, actualice el archivo `/etc/hosts` local con los FQDN de Harbor y Notary asignados a la dirección `External-IP` del equilibrador de carga; por ejemplo:

```
127.0.0.1 localhost
127.0.1.1 ubuntu
# TKGS Harbor with Envoy Load Balancer IP
10.195.141.17 core.harbor.domain
10.195.141.17 core.notary.harbor.domain
```

3 Para comprobar la instalación de la extensión Harbor, inicie sesión en Harbor. Consulte Iniciar sesión en la interfaz web de Harbor.

4 Cree dos registros CNAME en un servidor DNS que asignen la dirección `External-IP` del servicio Envoy del equilibrador de carga al FQDN de Harbor y al FQDN de Notary.

5 Instale la extensión DNS externo. Consulte Implementar y administrar la extensión TKG para la detección de servicios de DNS externos.

Configurar DNS para Harbor mediante un servicio Envoy de tipo NodePort (redes de vDS)

Si el servicio Envoy de requisitos previos se expone a través de NodePort, obtenga la dirección IP de la máquina virtual de un nodo de trabajo y cree registros de DNS para los FQDN de Harbor.

Nota Para usar NodePort, debe haber especificado el valor de `port.https` correcto en el archivo `harbor-data-values.yaml`.

1 Cambie el contexto a la instancia de espacio de nombres de vSphere en la que se aprovisiona el clúster.

```
kubectl config use-context VSPHERE-NAMESPACE
```

2 Enumere los nodos del clúster.

```
kubectl get virtualmachines
```

Debería ver los nodos del clúster; por ejemplo:

```
NAME                                           POWERSTATE   AGE
tkgs-cluster-X-control-plane-6dgln             poweredOn    6h7m
tkgs-cluster-X-control-plane-j6hq6             poweredOn    6h10m
tkgs-cluster-X-control-plane-xc25f             poweredOn    6h14m
tkgs-cluster-X-workers-9twdr-59bc54dc97-kt4cm  poweredOn    6h12m
tkgs-cluster-X-workers-9twdr-59bc54dc97-pjptr  poweredOn    6h12m
tkgs-cluster-X-workers-9twdr-59bc54dc97-t45mn  poweredOn    6h12m
```

3 Seleccione uno de los nodos de trabajo y describa el nodo mediante el siguiente comando.

```
kubectl describe virtualmachines tkgs-cluster-X-workers-9twdr-59bc54dc97-kt4cm
```

4 Busque la dirección IP de la máquina virtual; por ejemplo, `Vm Ip: 10.115.22.43`.

5 Para comprobar la instalación de la extensión Harbor, actualice el archivo `/etc/hosts` local con los FQDN de Harbor y Notary asignados a la dirección IP del nodo de trabajo; por ejemplo:

```
127.0.0.1 localhost
127.0.1.1 ubuntu
# TKGS Harbor with Envoy NodePort
10.115.22.43 core.harbor.domain
10.115.22.43 core.notary.harbor.domain
```

6 Para comprobar la instalación de la extensión Harbor, inicie sesión en Harbor. Consulte Iniciar sesión en la interfaz web de Harbor.

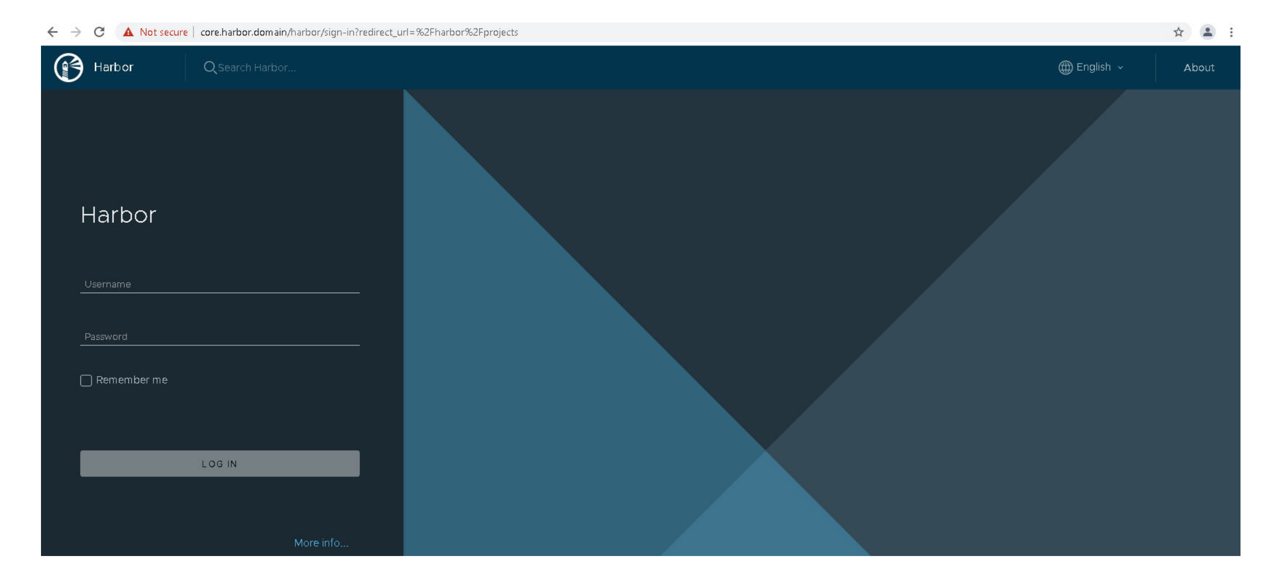
7 Cree dos registros CNAME en un servidor DNS que asignen la dirección IP del nodo de trabajo al FQDN de Harbor y al FQDN de Notary.

8 Instale la extensión DNS externo. Consulte Implementar y administrar la extensión TKG para la detección de servicios de DNS externos.

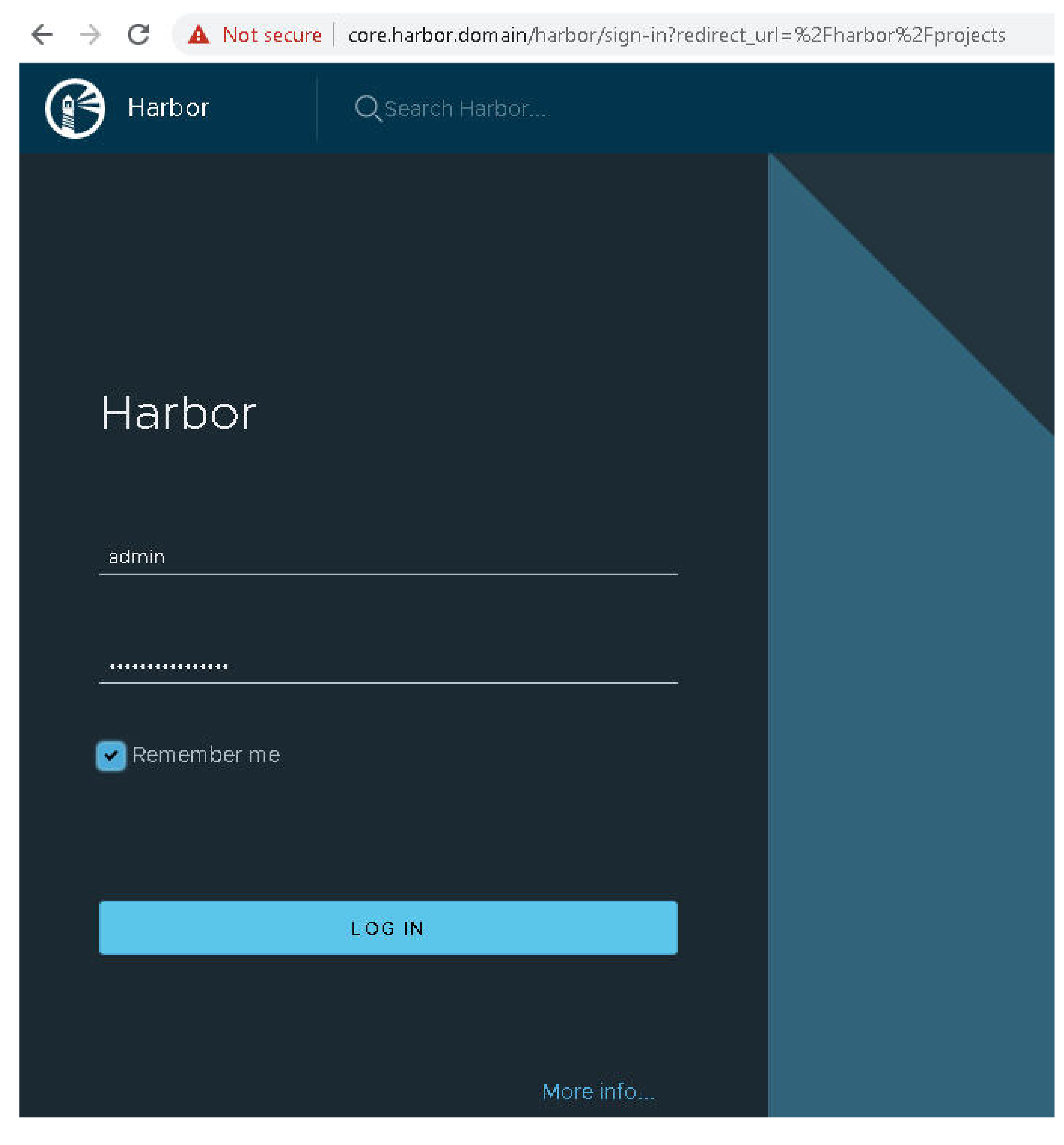
Iniciar sesión en la interfaz web de Harbor

Una vez que Harbor esté instalado y configurado, inicie sesión y comience a utilizarlo.

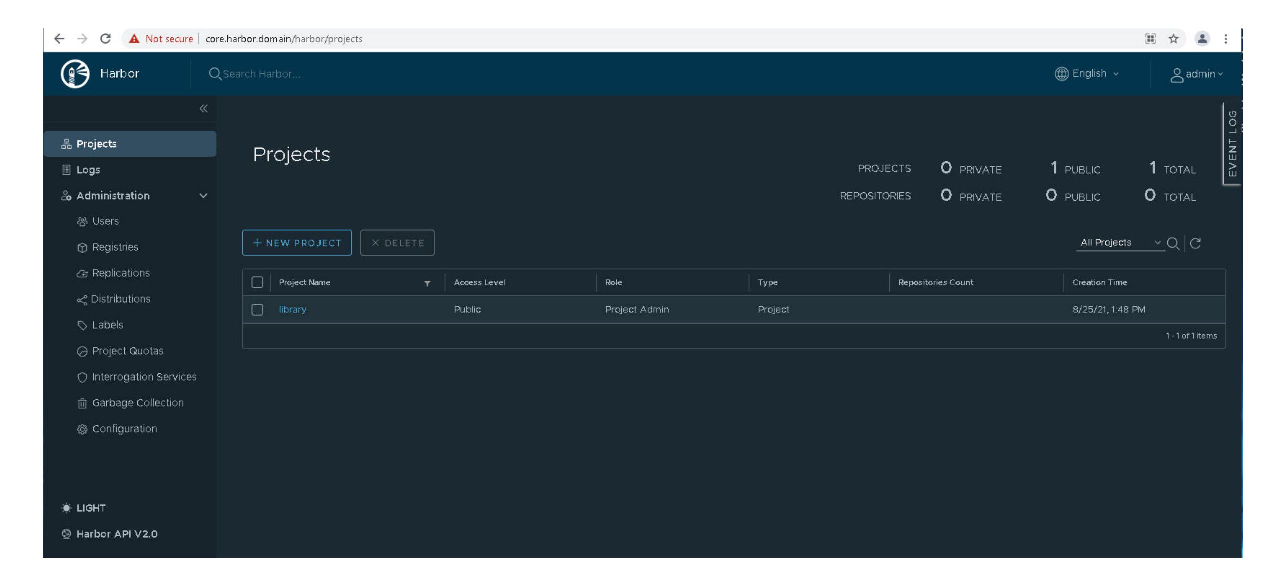
1 Acceda a la interfaz web del registro de Harbor en https://core.harbor.domain o al nombre de host que utilizó.



2 Inicie sesión en Harbor con el nombre de usuario **`admin`** y la contraseña generada que colocó en el archivo `harbor-data-values.yaml`.



3 Compruebe que puede acceder a la interfaz de usuario de Harbor.



4 Obtenga el certificado de CA de Harbor.

En la interfaz de Harbor, seleccione **Proyectos > biblioteca** o cree un **Nuevo proyecto**.

Haga clic en **Certificado del registro** y descargue el certificado de CA de Harbor (`ca.crt`).

5 Agregue el certificado de CA de Harbor al almacén de confianza del cliente de Docker para poder insertar y extraer imágenes de contenedor al registro de Harbor y desde él. Consulte Configurar un cliente de Docker con un certificado de registro de Harbor integrado.

6 Consulte la documentación de Harbor para obtener más información sobre el uso de Harbor.

Solucionar problemas generados en la implementación del registro de Harbor

Si se produce un error en la implementación o la reconciliación, ejecute `kubectl get pods -n tanzu-system-registry` para ver el estado del pod. Los pods de `harbor` deben tener el estado `Running`. Si el estado de un pod es `ImagePullBackOff` o `ImageCrashLoopBackOff`, no se podrá extraer la imagen del contenedor. Compruebe la URL del registro en los valores de datos y los archivos YAML de extensión, y asegúrese de que sean precisos.

Compruebe los registros del contenedor, en los que `name-XXXX` es el nombre único del pod cuando ejecuta `kubectl get pods -A`:

```
kubectl logs pod/harbor-XXXXX -c harbor -n tanzu-system-registry
```

Actualizar la extensión Harbor

Actualice la extensión de Contour que está implementada en el clúster de Tanzu Kubernetes.

1 Obtenga los valores de datos de Harbor del secreto.

```
kubectl get secret harbor-data-values -n tanzu-system-registry -o 'go-
template={{ index .data "values.yaml" }}' | base64 -d > harbor-data-values.yaml
```

2 Actualice los valores de datos de Harbor en `harbor-data-values.yaml`.

3 Actualice el secreto de los valores de datos de Harbor.

```
kubectl create secret generic harbor-data-values --from-file=values.yaml=harbor-data-values.yaml -n tanzu-system-registry -o yaml --dry-run | kubectl replace -f-
```

La extensión Harbor se conciliará con los nuevos valores de datos.

Nota De forma predeterminada, kapp-controller sincronizará las aplicaciones cada 5 minutos. La actualización debería tener efecto en 5 minutos o menos. Si desea que la actualización se aplique inmediatamente, cambie los valores de `syncPeriod` en `harbor-extension.yaml` a un valor menor y aplique la extensión de Contour mediante `kubectl apply -f harbor-extension.yaml`.

4 Compruebe el estado de la extensión.

```
kubectl get app harbor -n tanzu-system-registry
```

El estado de la aplicación Contour debe cambiar a `Reconcile Succeeded` una vez que Contour se actualice.

5 Vea el estado detallado y solucione los problemas.

```
kubectl get app harbor -n tanzu-system-registry -o yaml
```

Eliminar la extensión Harbor

Elimine la extensión Harbor de un clúster de Tanzu Kubernetes.

Nota Complete los pasos en orden. No elimine los objetos de función y espacio de nombres Contour antes de eliminar la aplicación y la extensión Contour. Al eliminar los objetos de función y espacio de nombres Contour, se elimina la cuenta de servicio que utiliza kapp-controller. Si esta cuenta de servicio se elimina antes de eliminar la aplicación y la extensión, se pueden producir errores en el sistema.

1 Cambie el directorio en el que descargó los archivos de la extensión Harbor.

```
cd /extensions/registry/harbor/
```

2 Elimine la aplicación Harbor.

```
kubectl delete app harbor -n tanzu-system-registry
```

Resultado esperado:

```
app.kappctrl.k14s.io "harbor" deleted
```

3 Compruebe que la aplicación Harbor se haya eliminado.

```
kubectl get app Harbor -n tanzu-system-registry
```

Resultado esperado: el estado de la aplicación es `Not Found`.

```
apps.kappctrl.k14s.io "harbor" not found
```

4 Elimine el espacio de nombres del registro.

Solo después de confirmar que la aplicación y la extensión Harbor se han eliminado completamente se pueden eliminar de forma segura los objetos de función y espacio de nombres.

```
kubectl delete -f namespace-role.yaml
```

Resultado esperado: se elimina el espacio de nombres donde está implementado Harbor y los objetos de control de acceso basado en funciones asociados.

```
namespace "tanzu-system-registry" deleted
serviceaccount "harbor-extension-sa" deleted
role.rbac.authorization.k8s.io "harbor-extension-role" deleted
rolebinding.rbac.authorization.k8s.io "harbor-extension-rolebinding" deleted
clusterrole.rbac.authorization.k8s.io "harbor-extension-cluster-role" deleted
clusterrolebinding.rbac.authorization.k8s.io "harbor-extension-cluster-rolebinding" deleted
```

Actualizar la extensión Harbor

Si tiene una extensión Harbor existente implementada, puede actualizarla a la versión más reciente.

1 Obtenga el mapa de configuración de Harbor.

```
kubectl get configmap harbor -n tanzu-system-harbor -o 'go-template={{ index .data
"harbor.yaml" }}' > harbor-configmap.yaml
```

2 Elimine la implementación de Harbor existente. Consulte Eliminar la extensión Harbor.

3 Implemente la extensión Harbor. Consulte Implementar la extensión Harbor.

Implementar y administrar la extensión TKG para la detección de servicios de DNS externos

El DNS externo permite configurar registros de DNS de forma dinámica en función de los servicios con carga equilibrada de Kubernetes. Puede implementar la extensión TKG para DNS externo a fin de proporcionar la detección dinámica de servicios para el clúster.

Requisitos previos de la extensión

Cumpla los siguientes requisitos antes de implementar la extensión TKG v1.3.1 para DNS externo.

- Aprovisionar un clúster de Tanzu Kubernetes. Consulte Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS.
- Conectarse al clúster de Tanzu Kubernetes. Consulte Conectarse a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.

- Descargar el paquete de extensiones TKG v1.3.1 Al host cliente en el que se ejecuta kubectl.
- Instalar los requisitos previos de las extensiones TKG en el clúster de Tanzu Kubernetes de destino.

Otros requisitos

Las configuraciones de muestra proporcionadas con la extensión DNS externo incluyen ejemplos con y sin el controlador de entrada de Contour. Si utiliza Contour, instálelo antes de instalar la extensión DNS externo. Consulte Implementar y administrar la extensión TKG para la entrada de Contour.

La extensión DNS externo permite la detección dinámica de servicios. Un caso de uso común es con el registro de Harbor. Harbor requiere una zona de DNS configurada en un proveedor de DNS dinámico compatible con RFC 2136, como AWS Route53, Azure DNS, Google Cloud DNS o un servidor DNS local como BIND. Consulte Implementar y administrar la extensión TKG para el registro de Harbor.

Implementar la extensión DNS externo

Complete los siguientes pasos antes de instalar la extensión TKG v1.3.1 para DNS externo.

1 Cambie el directorio en el que descargó los archivos de la extensión DNS externo.

```
cd /tkg-extensions-v1.3.1+vmware.1/extensions/service-discovery/external-dns
```

2 Cree el espacio de nombres y varios objetos de control de acceso basado en funciones para usarlos con la extensión DNS externo.

```
kubectl apply -f namespace-role.yaml
```

Este comando crea el espacio de nombres `tanzu-system-service-discovery` y los objetos RBAC asociados. Ejecute `kubect get ns` para comprobarlos.

3 Cree un archivo de valores de datos. El archivo de valores de datos de ejemplo proporciona la configuración mínima que se pide.

Hay archivos de valores de datos de ejemplo para AWS, Azure y un proveedor de DNS dinámico compatible con RFC 2136; cada uno con y sin entrada de Contour. Elija el archivo de ejemplo adecuado y cópielo.

Por ejemplo, si utiliza AWS Route 53 con Contour, ejecute el siguiente comando.

```
cp external-dns-data-values-aws-with-contour.yaml.example external-dns-data-values-aws-
with-contour.yaml
```

O bien, si utiliza Azure con Contour, ejecute el siguiente comando.

```
cp external-dns-data-values-azure-with-contour.yaml.example external-dns-data-values-azure-
with-contour.yaml
```

4 Configure los valores de datos de DNS externos.

Por ejemplo, a continuación se muestra la configuración de DNS de Azure. Proporcione los valores de `domain-filter` y `azure-resource-group`.

```
#@data/values
#@overlay/match-child-defaults missing_ok=True
---
externalDns:
  image:
    repository: projects.registry.vmware.com/tkg
  deployment:
    #@overlay/replace
    args:
    - --provider=azure
    - --source=service
    - --source=ingress
    - --domain-filter=my-zone.example.org #! zone where services are deployed
    - --azure-resource-group=my-resource-group #! Azure resource group
    #@overlay/replace
    volumeMounts:
    - name: azure-config-file
      mountPath: /etc/kubernetes
      readOnly: true
    #@overlay/replace
    volumes:
    - name: azure-config-file
      secret:
        secretName: azure-config-file
```

5 Cree un secreto genérico con el archivo de valores de datos que ha rellenado.

Por ejemplo, el siguiente comando crea el secreto mediante el archivo de valores de datos DNS de Azure.

```
kubectl create secret generic external-dns-data-values --from-file=values.yaml=external-
dns-data-values-azure-with-contour.yaml -n tanzu-system-service-discovery
```

Debería ver que `secret/external-dns-data-values created` se ha creado en el espacio de nombres `tanzu-system-service-discovery`. Puede verificarlo con el comando `kubectl get secrets -n tanzu-system-service-discovery`.

6 Implemente la extensión DNS externo.

```
kubectl apply -f external-dns-extension.yaml
```

Si todo es correcto, debería ver `app.kappctrl.k14s.io/external-dns created`.

7 Compruebe el estado de la implementación de la extensión.

```
kubectl get app external-dns -n tanzu-system-service-discovery
```

El estado de la aplicación debe cambiar de `Reconciling` a `Reconcile succeeded` una vez que DNS externo se implemente correctamente. Si el estado es `Reconcile failed`, consulte Solucionar problemas de la implementación.

8 Ver estado detallado.

```
kubectl get app external-dns -n tanzu-system-service-discovery -o yaml
```

Solucionar problemas de la implementación

Si se produce un error en la reconciliación, ejecute el comando `kubectl get pods -A` para ver el estado de los pods. En condiciones normales, debería ver que el estado del pod `external-dns-XXXXX` es `Running`. Si se produce un error en la reconciliación o el estado del pod es `ImagePullBackOff` o `ImagecRashLoopBackOff`, quiere decir que no se pudo extraer la imagen del contenedor del repositorio. Compruebe la dirección URL del repositorio en los valores de datos y los archivos YAML de extensión, y asegúrese de que sean precisos.

Para comprobar los registros del contenedor, ejecute los siguientes comandos, donde `name-XXXX` es el nombre único del pod que puede ver cuando ejecuta `kubectl get pods -A`:

```
kubectl logs pod/external-dns-XXXXX -c external-dns -n tanzu-system-service-discovery
```

Actualizar la extensión DNS externo

Actualice la extensión DNS externo que está implementada en el clúster de Tanzu Kubernetes.

1 Obtenga los valores de datos de Contour del secreto.

```
kubectl get secret external-dns-data-values -n tanzu-system-service-discovery -o 'go-
template={{ index .data "values.yaml" }}' | base64 -d > external-dns-data-values.yaml
```

2 Actualice los valores de datos de DNS externo en `external-dns-data-values.yaml`. Consulte Configurar la extensión DNS externo.

3 Actualice el secreto de los valores de datos de Contour.

```
kubectl create secret generic external-dns-data-values --from-file=values.yaml=external-
dns-data-values.yaml -n tanzu-system-service-discovery -o yaml --dry-run | kubectl replace
-f-
```

La extensión DNS externo se conciliará con los nuevos valores de datos.

Nota De forma predeterminada, kapp-controller sincronizará las aplicaciones cada 5 minutos. La actualización debería tener efecto en 5 minutos o menos. Si desea que la actualización se aplique inmediatamente, cambie los valores de `syncPeriod` en `external-dns-extension` a un valor menor y aplique la extensión de Contour mediante `kubectl apply -f external-dns-extension`.

4 Compruebe el estado de la extensión.

```
kubectl get app external-dns -n tanzu-system-service-disovery
```

El estado de la aplicación debe cambiar a `Reconcile Succeeded` una vez que se actualice.

5 Vea el estado detallado y solucione los problemas.

```
kubectl get app external-dns -n tanzu-system-service-disovery -o yaml
```

Eliminar la extensión DNS externo

Elimine la extensión DNS externo de un clúster de Tanzu Kubernetes.

Nota Complete los pasos en orden. No elimine los objetos de función ni el espacio de nombres de destino antes de eliminar la aplicación y la extensión. Al eliminar el espacio de nombres y los objetos de función, se elimina la cuenta de servicio que utiliza kapp-controller. Si esta cuenta de servicio se elimina antes de eliminar la aplicación y la extensión, se pueden producir errores en el sistema.

1 Cambie el directorio en el que descargó los archivos de la extensión.

```
cd /tkg-extensions-v1.3.1+vmware.1/extensions/service-discovery/external-dns
```

2 Elimine la extensión DNS externo.

```
kubectl delete -f external-dns-extension.yaml
```

3 Compruebe que la extensión se haya eliminado.

```
kubectl get app contour -n tanzu-system-ingress
```

Resultado esperado: el estado de la aplicación es `Not Found`.

4 Elimine el espacio de nombres.

Solo después de confirmar que la aplicación y la extensión Contour se han eliminado completamente se pueden eliminar de forma segura los objetos de función y espacio de nombres.

```
kubectl delete -f namespace-role.yaml
```

Resultado esperado: se elimina el espacio de nombres donde está implementada la extensión y los objetos de control de acceso basado en funciones asociados.

Configurar la extensión DNS externo

La extensión DNS externo se puede configurar con parámetros personalizados.

Configure los parámetros de implementación para el proveedor de DNS externo. Consulte el sitio de Kubernetes https://github.com/kubernetes-sigs/external-dns#running-externaldns para obtener más instrucciones.

Tabla 14-10. Parámetros de configuración de la extensión Harbor

Parámetro	Descripción	Tipo	Predeterminado
externalDns.namespace	Espacio de nombres en el que se implementará el DNS externo	string	tanzu-system-service-discovery
externalDns.image.repository	Repositorio que contiene la imagen de DNS externo	string	projects.registry.vmware.com/tkg
externalDns.image.name	Nombre de external-dns	string	external-dns
externalDns.image.tag	Etiqueta de la imagen de DNS externo	string	v0.7.4_vmware.1
externalDns.image.pullPolicy	Directiva de extracción de la imagen de DNS externo	string	IfNotPresent
externalDns.deployment.annotations	Anotaciones en la implementación de external-dns	map<string,string>	{}
externalDns.deployment.args	Argumentos transmitidos a través de la línea de comandos a external-dns	list<string>	[] (parámetro obligatorio)
externalDns.deployment.env	Variables de entorno que se transferirán a external-dns	list<string>	[]
externalDns.deployment.securityContext	Contexto de seguridad del contenedor de DNS externo	SecurityContext	{}
externalDns.deployment.volumeMounts	Montajes de volumen del contenedor de external-dns	list<VolumeMount>	[]
externalDns.deployment.volumes	Volúmenes del pod de DNS externo	list<Volume>	[]

Implementar cargas de trabajo de AI/ML en clústeres de Tanzu Kubernetes

Puede implementar cargas de trabajo de AI/ML en clústeres de Tanzu Kubernetes aprovisionados por servicio Tanzu Kubernetes Grid. La implementación de cargas de trabajo de AI/ML requiere una configuración inicial por parte del administrador de vSphere y una configuración por parte del operador del clúster. Una vez que el entorno de vSphere with Tanzu está habilitado para vGPU, los desarrolladores pueden implementar cargas de trabajo de AI/ML en sus clústeres TKGS de la misma manera que lo harían con cualquier otra carga de trabajo de Kubernetes.

Acerca de la implementación de cargas de trabajo de AI/ML en clústeres TKGS

Las cargas de trabajo de AI/ML se pueden implementar en clústeres TKGS mediante vSphere with Tanzu y la tecnología vGPU de NVIDIA.

Anuncio de la compatibilidad con TGKS para cargas de trabajo de AI/ML

A partir del lanzamiento de vSphere with Tanzu versión 7 Update 3, revisión mensual 1, puede implementar cargas de trabajo de uso intensivo de recursos informáticos en los clústeres de Tanzu Kubernetes aprovisionados por servicio Tanzu Kubernetes Grid. En este contexto, una carga de trabajo con uso intensivo de recursos informáticos es una aplicación de inteligencia artificial (AI) o aprendizaje automático (ML) que requiere el uso de un dispositivo acelerador de GPU.

Para facilitar la ejecución de cargas de trabajo de AI/ML en un entorno de Kubernetes, VMware se asocia con NVIDIA para admitir la plataforma GPU Cloud de NVIDIA en vSphere with Tanzu. Esto significa que puede implementar imágenes de contenedor desde el catálogo de NGC en clústeres de Tanzu Kubernetes aprovisionados por servicio Tanzu Kubernetes Grid.

Para obtener más información sobre la arquitectura conjunta de NVIDIA y VMware para la empresa lista para AI, consulte Acelerar cargas de trabajo en vSphere 7 with Tanzu: una vista previa técnica de clústeres de Kubernetes con GPU.

Modos vGPU compatibles

La implementación de cargas de trabajo de AI/ML en TKGS requiere el uso del archivo OVA de Ubuntu que está disponible a través de la red de entrega de contenido de vSphere with Tanzu. TKGS admite dos modos de operaciones de GPU: vGPU y vGPU con acceso directo a la NIC. En la tabla se describen los dos modos con más detalles.

Modo	Configuración	Descripción
NVIDIA + TKGS + Ubuntu + vGPU	vGPU de NVIDIA	El controlador del administrador de hosts NVIDIA instalado en cada host ESXi virtualiza el dispositivo GPU. Este se comparte después entre varias GPU virtuales (vGPU) de NVIDIA. Cada vGPU de NVIDIA se define por la cantidad de memoria del dispositivo GPU. Por ejemplo, si el dispositivo GPU tiene una cantidad total de 32 GB de RAM, puede crear 8 vGPU con aproximadamente 4 GB de memoria cada uno.
NVIDIA + TKGS + Ubuntu + vGPU + acceso directo a la NIC	vGPU de NVIDIA **y** Instancia dinámica de DirectPath I/O	En la misma clase de máquina virtual en la que se configura el perfil de la vGPU de NVIDIA, se incluye compatibilidad con un dispositivo de redes de acceso directo mediante la instancia dinámica de DirectPath I/O. En este caso, vSphere DRS determina la colocación de máquinas virtuales.

Introducción

Para configurar la vGPU de NVIDIA para TKGS, consulte los siguientes temas:

- Flujo de trabajo del administrador de vSphere para implementar cargas de trabajo de AI/ML en clústeres TKGS (vGPU)
- Flujo de trabajo de operadores de clúster para implementar cargas de trabajo de AI/ML en clústeres TKGS

Si utiliza la vGPU con acceso directo a la NIC, consulte también el siguiente tema: Anexo del administrador de vSphere para implementar cargas de trabajo de AI/ML en clústeres TKGS (vGPU e Instancia dinámica de DirectPath I/O).

Si utiliza el servidor de licencias delegado (DLS) de NVIDIA para su cuenta de NVAIE, consulte también el siguiente tema: Anexo de operadores de clúster para implementar cargas de trabajo de AI/ML en clústeres TKGS (DLS).

Flujo de trabajo del administrador de vSphere para implementar cargas de trabajo de AI/ML en clústeres TKGS (vGPU)

Para permitir que los desarrolladores implementen cargas de trabajo de AI/ML en clústeres TKGS, como administrador de vSphere, configure el entorno de vSphere with Tanzu para que admita el hardware de NVIDIA GPU.

Flujo de trabajo del administrador de vSphere para implementar cargas de trabajo de AI/ML en clústeres TKGS

El flujo de trabajo de alto nivel para que administradores de vSphere permitan la implementación de cargas de trabajo de AI/ML en clústeres TKGS se muestra en la tabla. A continuación se indican instrucciones detalladas para cada paso.

Paso	Acción	Vincular
0	Revise los requisitos del sistema.	Consulte Paso 0 del administrador: Revisar los requisitos del sistema.
1	Instale un dispositivo NVIDIA GPU compatible en hosts ESXi.	Consulte Paso 1 del administrador: Instalar un dispositivo NVIDIA GPU compatible en hosts ESXi.
2	Configure los ajustes de gráficos de dispositivos ESXi para las operaciones de vGPU.	Consulte Paso 2 del administrador: Configurar cada host ESXi para operaciones de vGPU.
3	Instale el administrador de NVIDIA vGPU (VIB) en cada host ESXi.	Consulte Paso 3 del administrador: Instalar el controlador del administrador de hosts de NVIDIA en cada host ESXi.
4	Compruebe la operación del controlador de NVIDIA y el modo de virtualización de GPU.	Consulte Paso 4 del administrador: Comprobar que los hosts ESXi estén listos para las operaciones de NVIDIA vGPU.

Paso	Acción	Vincular
5	Habilite la administración de cargas de trabajo en el clúster configurado para GPU. El resultado es un clúster supervisor que se ejecuta en hosts ESXi habilitados para vGPU.	Consulte Paso 5 del administrador: Habilitar la administración de cargas de trabajo en el clúster de vCenter configurado para vGPU.
6	Cree* o actualice una biblioteca de contenido para las versiones de Tanzu Kubernetes y rellene la biblioteca con el archivo OVA de Ubuntu compatible que se requiere para las cargas de trabajo de vGPU.	Consulte Paso 6 del administrador: Crear o actualizar una biblioteca de contenido con la versión de Ubuntu para Tanzu Kubernetes. **Nota** *Si es necesario. Si ya tiene una biblioteca de contenido para imágenes Photon de clústeres de TKGS, no cree una biblioteca de contenido nueva para imágenes de Ubuntu.
7	Cree una clase de máquina virtual personalizada con un determinado perfil de vGPU seleccionado.	Consulte Paso 7 del administrador: Crear una clase de máquina virtual personalizada con el perfil de vGPU.
8	Cree y configure un espacio de nombres de vSphere para clústeres GPU de TKGS: agregue un usuario con permisos de edición y almacenamiento para volúmenes persistentes.	Consulte Paso 8 de administración: Crear y configurar un espacio de nombres de vSphere para el clúster GPU de TKGS.
9	Asocie la biblioteca de contenido con el archivo OVA de Ubuntu y la clase de máquina virtual personalizada para vGPU con el espacio de nombres de vSphere que creó para TGKS.	Consulte Paso 9 del administrador: Asociar la biblioteca de contenido y la clase de máquina virtual con el espacio de nombres de vSphere.
10	Compruebe que se aprovisione el clúster supervisor y que el operador del clúster pueda acceder a él.	Consulte Paso 10 del administrador: comprobar que se pueda acceder al clúster supervisor.

Paso 0 del administrador: Revisar los requisitos del sistema

Consulte los siguientes requisitos del sistema para configurar el entorno de implementación de cargas de trabajo de AI/ML en clústeres TKGS.

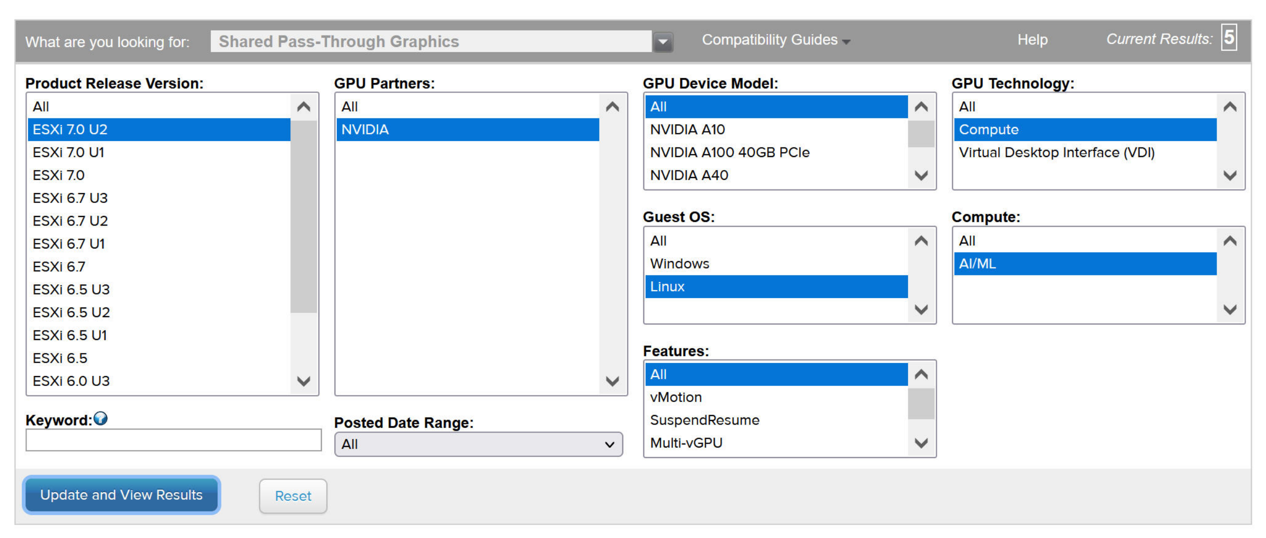
Requisito	Descripción
Infraestructura de vSphere	vSphere 7 Update3, revisión mensual 1 ESXi compilación `18778458` o posterior vCenter Server compilación `18644231` o posterior
Administración de cargas de trabajo	Versión de espacio de nombres de vSphere `0.0.11-18610518` o posterior
Clúster supervisor	Versión de clúster supervisor `v1.21.0+vmware.1-vsc0.0.11-18610518` o posterior
OVA de TKR Ubuntu	versión de Tanzu Kubernetes Ubuntu `ob-18691651-tkgs-ova-ubuntu-2004-v1.20.8---vmware.1-tkg.2`

Requisito	Descripción
Controlador de host NVIDIA vGPU	Descargue el VIB del sitio web de NGC. Si desea más información, consulte la documentación del controlador del software vGPU. Por ejemplo: `NVIDIA-AIE_ESXi_7.0.2_Driver_470.51-1OEM.702.0.0.17630552.vib`
Servidor de licencias NVIDIA para vGPU	FQDN proporcionado por la organización

Paso 1 del administrador: Instalar un dispositivo NVIDIA GPU compatible en hosts ESXi

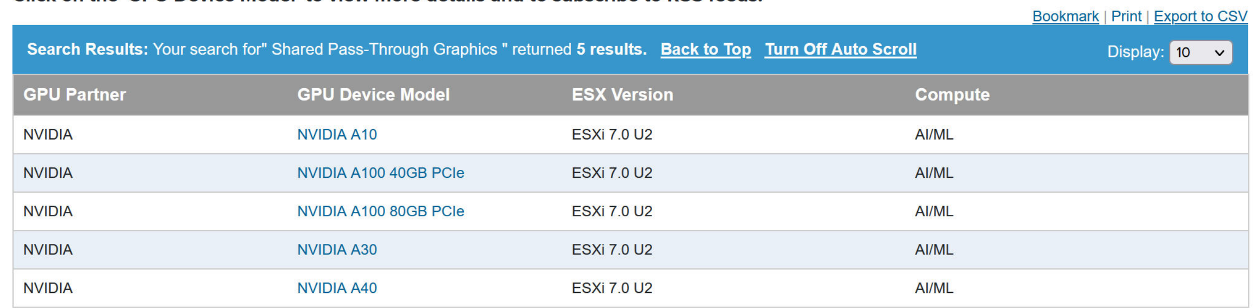
Para implementar cargas de trabajo de AI/ML en TKGS, instale uno o varios dispositivos NVIDIA GPU compatibles en cada host ESXi que contenga el clúster de vCenter en el que se habilitará **Administración de cargas de trabajo**.

Para ver los dispositivos NVIDIA GPU compatibles, consulte la guía de compatibilidad de VMware.



Click here to **Read** Important Support Information

Click on the 'GPU Device Model' to view more details and to subscribe to RSS feeds.



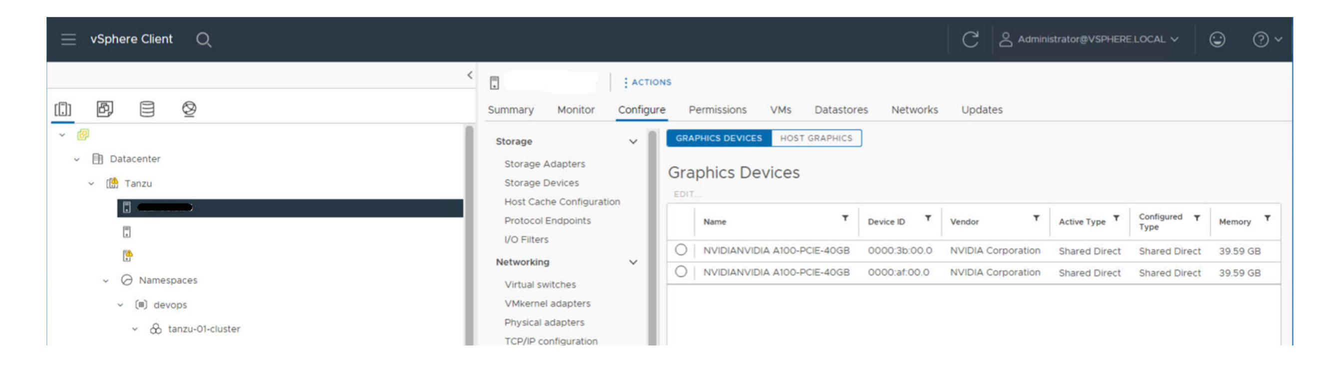
Bookmark | Print | Export to CSV

Search Results: Your search for" Shared Pass-Through Graphics " returned **5 results.** Back to Top Turn Off Auto Scroll Display: 10

GPU Partner	GPU Device Model	ESX Version	Compute
NVIDIA	NVIDIA A10	ESXi 7.0 U2	AI/ML
NVIDIA	NVIDIA A100 40GB PCIe	ESXi 7.0 U2	AI/ML
NVIDIA	NVIDIA A100 80GB PCIe	ESXi 7.0 U2	AI/ML
NVIDIA	NVIDIA A30	ESXi 7.0 U2	AI/ML
NVIDIA	NVIDIA A40	ESXi 7.0 U2	AI/ML

El dispositivo NVIDIA GPU debe admitir los perfiles de vGPU NVIDIA AI Enterprise (NVAIE) más recientes. Consulte la documentación de GPU compatibles con el software NVIDIA Virtual GPU para obtener instrucciones.

Por ejemplo, el siguiente host ESXi tiene dos dispositivos NVIDIA GPU A100 instalados.



Paso 2 del administrador: Configurar cada host ESXi para operaciones de vGPU

Configure cada host ESXi para vGPU habilitando Compartidos directos y SR-IOV.

Habilitar Compartidos directos en cada host ESXi

Para que la funcionalidad NVIDIA vGPU se desbloquee, habilite el modo **Compartidos directos** en cada host ESXi que contenga el clúster de vCenter en el que se habilitará **Administración de cargas de trabajo**.

Para habilitar **Compartidos directos**, realice los siguientes pasos. Para obtener más instrucciones, consulte Configurar dispositivos de gráficos en la documentación de vSphere.

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Seleccione un host ESXi en el clúster de vCenter.

3 Seleccione **Configurar > Hardware > Gráficos**.

4 Seleccione el dispositivo acelerador de NVIDIA GPU.

5 **Edite** la configuración de dispositivos de gráficos.

6 Seleccione **Compartidos directos**.

7 Seleccione **Reiniciar el servidor X.Org**.

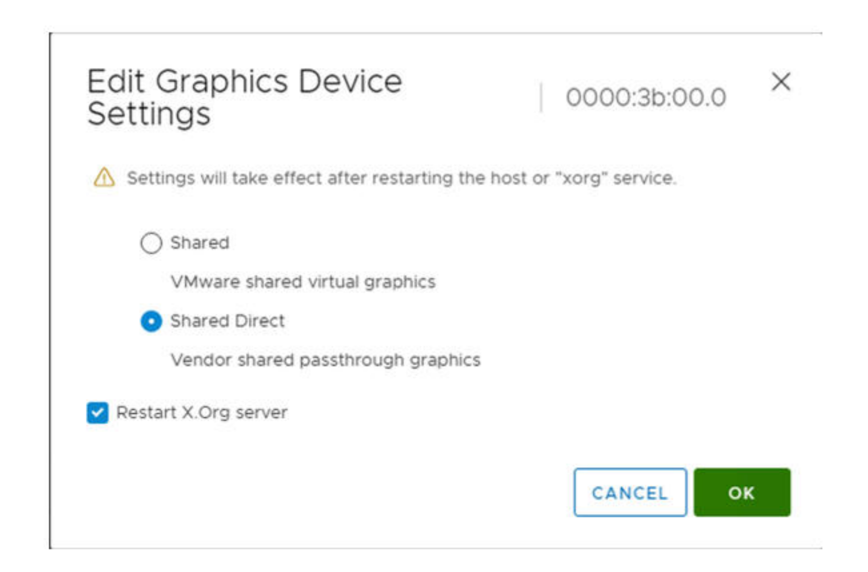
8 Haga clic en **Aceptar** para guardar la configuración.

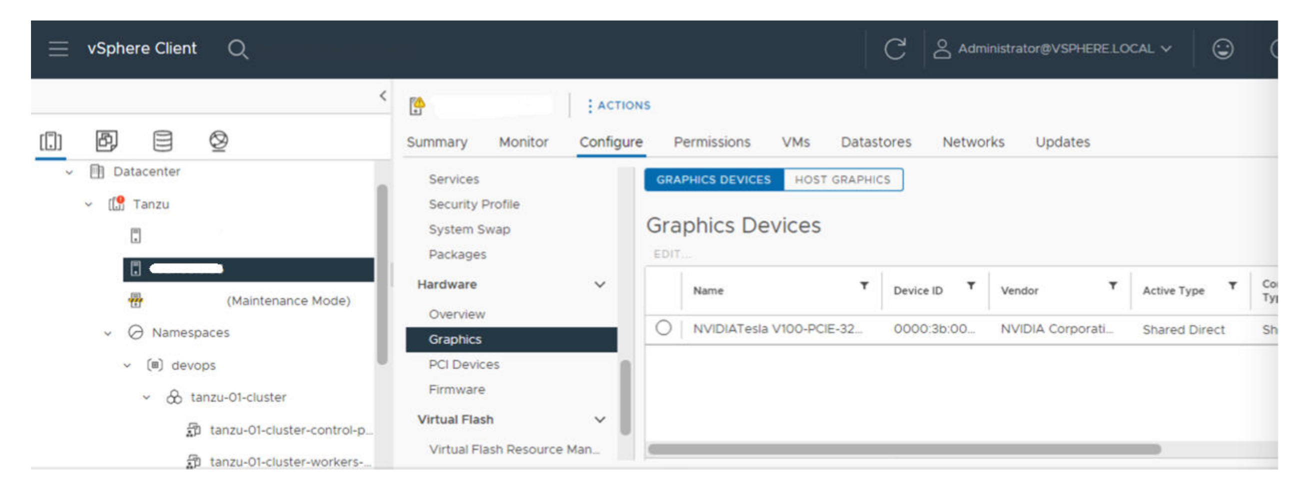
9 Haga clic con el botón secundario en el host ESXi y póngalo en el modo de mantenimiento.

10 Reinicie el host.

11 Cuando el host vuelva a ejecutarse, salga del modo de mantenimiento.

12 Repita este proceso para cada host ESXi en el clúster de vCenter en el que se habilitará **Administración de cargas de trabajo**.





Activar el BIOS de SR-IOV para dispositivos NVIDIA GPU A30 y A100

Si utiliza los dispositivos GPU NVIDIA A30 o A100, los cuales son necesarios para GPU de varias instancias (modo MIG), debe habilitar SR-IOV en el host ESXi. Si SR-IOV no está habilitado, no se pueden iniciar las máquinas virtuales del nodo del clúster de Tanzu Kubernetes. Si esto ocurre, verá el siguiente mensaje de error en el panel **Tareas recientes** de vCenter Server en el que está habilitada **Administración de cargas de trabajo**.

```
Could not initialize plugin libnvidia-vgx.so for vGPU nvidia_aXXX-xx. Failed to start
the virtual machine. Module DevicePowerOn power on failed.
```

Para habilitar SR-IOV, inicie sesión en el host ESXi mediante la consola web. Seleccione **Administrar > Hardware** . Seleccione el dispositivo NVIDIA GPU y haga clic en **Configurar SR-IOV**. Desde ahí, puede activar SR-IOV. Para ver más instrucciones, consulte Single Root I/O Virtualization (SR-IOV) en la documentación de vSphere.

Nota Si utiliza vGPU con acceso directo a la NIC, consulte el siguiente tema para obtener un paso adicional de configuración de ESXi: Anexo del administrador de vSphere para implementar cargas de trabajo de AI/ML en clústeres TKGS (vGPU e Instancia dinámica de DirectPath I/O).

Paso 3 del administrador: Instalar el controlador del administrador de hosts de NVIDIA en cada host ESXi

Para ejecutar las máquinas virtuales del nodo del clúster de Tanzu Kubernetes con aceleración de gráficos NVIDIA vGPU, instale el controlador del administrador de hosts de NVIDIA en cada host ESXi que contenga el clúster de vCenter en el que se habilitará **Administración de cargas de trabajo**.

Los componentes del controlador del administrador de hosts NVIDIA vGPU se empaquetan en un paquete de instalación de vSphere (VIB). La organización le proporciona el VIB de NVAIE a través de su programa de licencias NVIDIA GRID. VMware no proporciona los VIB de NVAIE ni hace que estén disponibles para descargarlos. Como parte del programa de licencias NVIDIA, su organización configura un servidor de licencias. Consulte la Guía de inicio rápido del software de GPU virtual para obtener más información.

Una vez que se configure el entorno de NVIDIA, ejecute el siguiente comando en cada host ESXi, reemplace la dirección del servidor de licencias NVIDIA y la versión del VIB de NVAIE con los valores adecuados para su entorno. Para obtener más instrucciones, consulte Instalar y configurar el VIB de NVIDIA en ESXi en la base de conocimientos de soporte de VMware.

Nota La versión del VIB de NVAIE instalada en los hosts ESXi debe coincidir con la versión de software de vGPU instalada en las máquinas virtuales del nodo. La siguiente versión es solo un ejemplo.

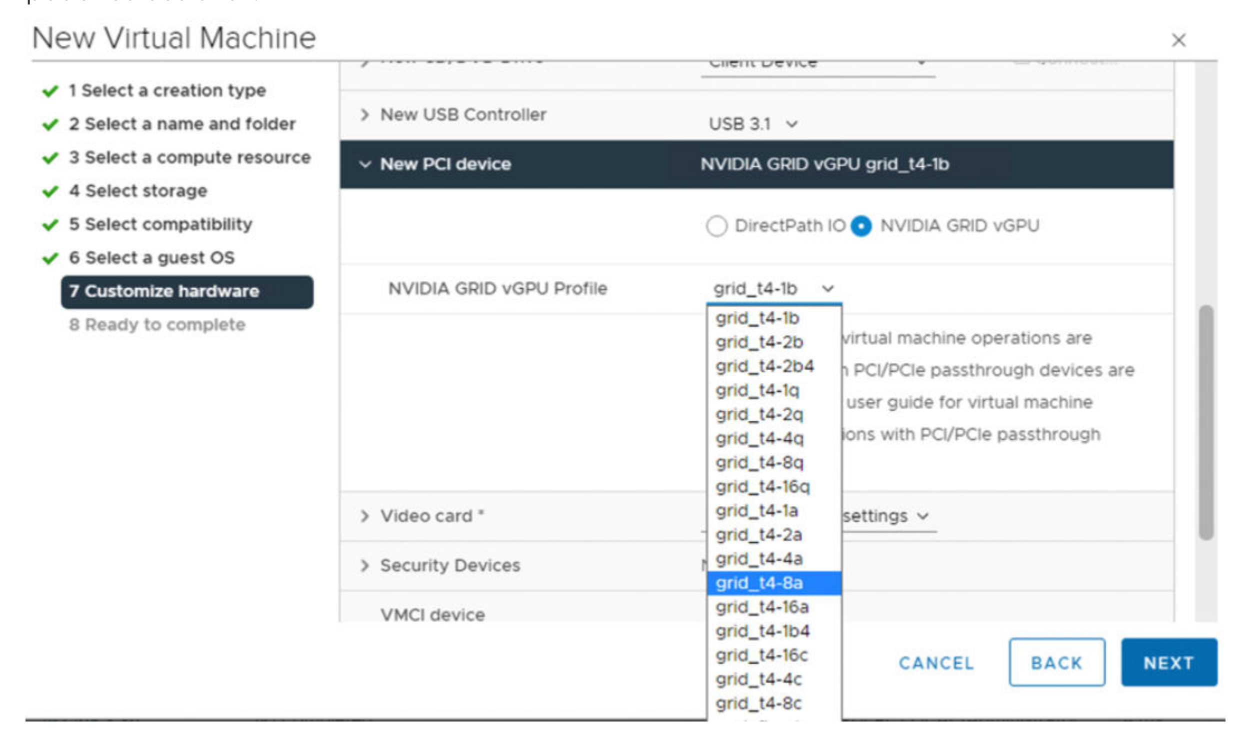
```
esxcli system maintenanceMode set --enable true
esxcli software vib install -v ftp://server.domain.example.com/nvidia/signed/
NVIDIA_bootbank_NVIDIA-VMware_ESXi_7.0_Host_Driver_460.73.02-1OEM.700.0.0.15525992.vib
esxcli system maintenanceMode set --enable false
/etc/init.d/xorg restart
```

Paso 4 del administrador: Comprobar que los hosts ESXi estén listos para las operaciones de NVIDIA vGPU

Para comprobar que cada host ESXi esté listo para las operaciones de NVIDIA vGPU, realice las siguientes comprobaciones en cada host ESXi del clúster de vCenter en el que se habilitará **Administración de cargas de trabajo**:

- Acceda mediante SSH al host ESXi, entre en el modo de shell y ejecute el comando `nvidia-smi`. La interfaz de administración del sistema NVIDIA es una utilidad de línea de comandos que proporciona el administrador de hosts de NVIDIA vGPU. Al ejecutar este comando, se devuelven los controladores y las GPU en el host.
- Ejecute el siguiente comando para comprobar que el controlador de NVIDIA esté instalado correctamente: `esxcli software vib list | grep NVIDA`.
- Compruebe que el host esté configurado con Compartidos directos de GPU y que SR-IOV esté activado (si utiliza dispositivos NVIDIA A30 o A100).

- Con vSphere Client, en el host ESXi que está configurado para GPU, cree una nueva máquina virtual con un dispositivo PCI incluido. El perfil de NVIDIA vGPU debe aparecer y se debe poder seleccionar.



Paso 5 del administrador: Habilitar la administración de cargas de trabajo en el clúster de vCenter configurado para vGPU

Ahora que los hosts ESXi están configurados para admitir NVIDIA vGPU, cree un clúster de vCenter que incluya estos hosts. Para admitir **Administración de cargas de trabajo**, el clúster de vCenter debe cumplir determinados requisitos, incluidos el almacenamiento compartido, la alta disponibilidad y el DRS completamente automatizado.

Para habilitar **Administración de cargas de trabajo**, también hay que seleccionar una pila de redes, ya sea de redes nativas de vSphere vDS o de redes de NSX-T Data Center. Si utiliza redes de vDS, debe instalar un equilibrador de carga, ya sea NSX Advanced o HAProxy.

El resultado de habilitar **Administración de cargas de trabajo** es un clúster supervisor que se ejecuta en los hosts ESXi habilitados para vGPU. Consulte las siguientes tareas y documentación para habilitar **Administración de cargas de trabajo**.

Nota Omita este paso si ya tiene un clúster de vCenter con **Administración de cargas de trabajo** habilitada, siempre que ese clúster utilice los hosts ESXi que configuró para vGPU.

Tarea	Instrucciones
Crear un clúster de vCenter que cumpla los requisitos para habilitar **Administración de cargas de trabajo**	Requisitos previos para configurar vSphere with Tanzu en un clúster de vSphere
Configure las redes del clúster supervisor, ya sea NSX-T o vDS con un equilibrador de carga.	Configurar NSX-T Data Center para vSphere with Tanzu. Configurar redes de vSphere y NSX Advanced Load Balancer para vSphere with Tanzu. Configurar redes de vSphere y el equilibrador de carga de HAProxy para vSphere with Tanzu.
Habilitar **Administración de cargas de trabajo**	Habilitar la administración de cargas de trabajo con redes de NSX-T Data Center. Habilitar la administración de cargas de trabajo con redes de vSphere.

Paso 6 del administrador: Crear o actualizar una biblioteca de contenido con la versión de Ubuntu para Tanzu Kubernetes

Una vez que **Administración de cargas de trabajo** esté habilitada en un clúster de vCenter configurado para GPU, el siguiente paso consiste en crear una biblioteca de contenido para la imagen OVA de la versión de Tanzu Kubernetes.

Advertencia Si ya tiene una biblioteca de contenido con versiones de Tanzu Kubernetes que constan de imágenes Photon, solo tiene que sincronizar la biblioteca de contenido existente con las imágenes de Ubuntu requeridas. No cree una segunda biblioteca de contenido para los clústeres de TKGS. Si lo hace, puede provocar inestabilidad en el sistema.

NVIDIA vGPU requiere el sistema operativo Ubuntu. VMware proporciona un archivo OVA de Ubuntu para estos fines. No es posible utilizar la versión de Tanzu Kubernetes para PhotonOS para clústeres de vGPU.

Para importar esta imagen en el entorno de vSphere with Tanzu, elija uno de los métodos que aparecen en la tabla y siga las instrucciones correspondientes.

Tipo de biblioteca de contenido	Descripción
Cree una **Biblioteca de contenido suscrita** y sincronice automáticamente el archivo OVA de Ubuntu con su entorno.	Crear, proteger y sincronizar una biblioteca de contenido suscrita para las versiones de Tanzu Kubernetes
Cree una **Biblioteca de contenido local** y cargue manualmente el archivo OVA de Ubuntu a su entorno.	Crear, proteger y sincronizar una biblioteca de contenido local para versiones de Tanzu Kubernetes

Cuando haya completado esta tarea, debería ver el archivo OVA de Ubuntu disponible en la biblioteca de contenido.



Paso 7 del administrador: Crear una clase de máquina virtual personalizada con el perfil de vGPU

El siguiente paso consiste en crear una clase de máquina virtual personalizada con un perfil de vGPU. El sistema utilizará esta definición de clase cuando cree los nodos del clúster de Tanzu Kubernetes.

Siga las instrucciones siguientes para crear una clase de máquina virtual personalizada con un perfil de vGPU. Para obtener más instrucciones, consulte Agregar dispositivos PCI a una clase de máquina virtual en vSphere with Tanzu.

Nota Si utiliza vGPU con acceso directo a la NIC, consulte el siguiente tema para obtener un paso adicional: Anexo del administrador de vSphere para implementar cargas de trabajo de AI/ML en clústeres TKGS (vGPU e Instancia dinámica de DirectPath I/O).

1 Inicie sesión en vCenter Server con vSphere Client.

2 Seleccione **Administración de cargas de trabajo**.

3 Seleccione **Servicios**

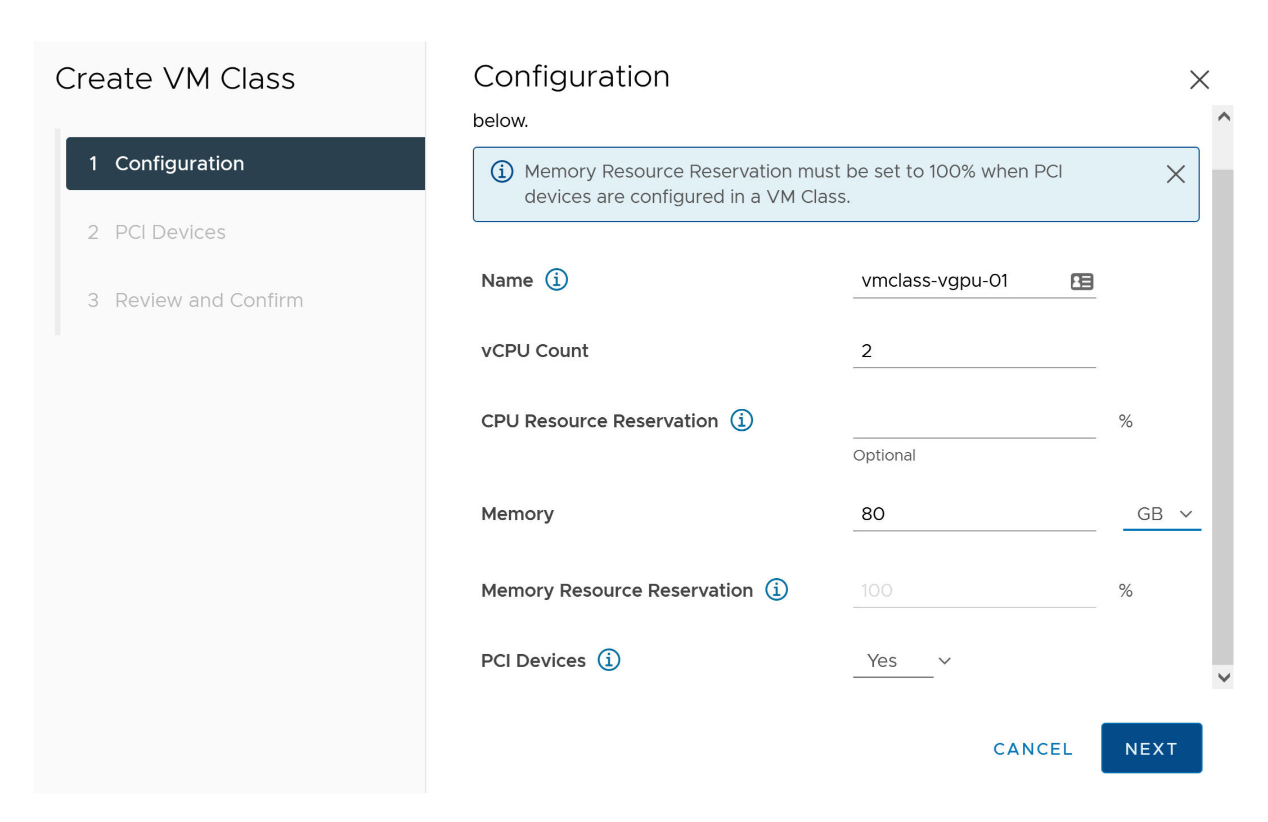
4 Seleccione **Clases de VM**.

5 Haga clic en **Crear clase de VM**.

6 En la pestaña **Configuración**, configure la clase de máquina virtual personalizada.

Campo de configuración	Descripción
Nombre	Introduzca un nombre descriptivo para la clase de máquina virtual personalizada, como `vmclass-vgpu-1`.
Recuento de vCPU	**2**
Reserva de recursos de CPU	Opcional, acepte para dejar en blanco
Memoria	**80 GB**, por ejemplo
Reserva de recursos de memoria	**100 %** (obligatorio cuando se configuran dispositivos PCI en una clase de máquina virtual)
Dispositivos PCI	**Sí** **Nota** Al seleccionar Sí para Dispositivos PCI, se indica al sistema que se utiliza un dispositivo GPU y se cambia la configuración de la clase de máquina virtual para admitir la configuración de vGPU.

Por ejemplo:



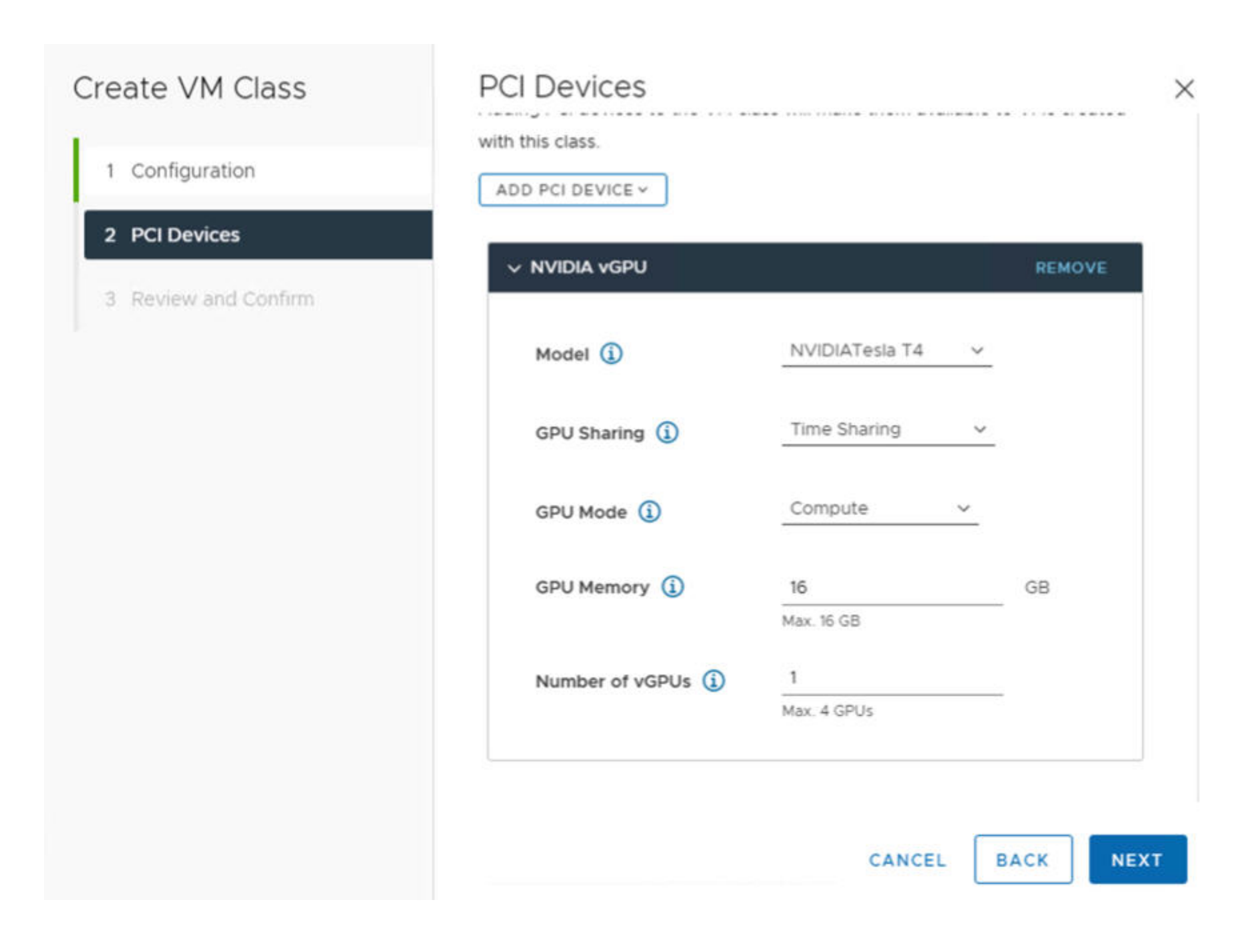
7 Haga clic en **Siguiente**.

8 En la pestaña **Dispositivos PCI**, seleccione la opción **Agregar dispositivo PCI > vGPU de NVIDIA**.

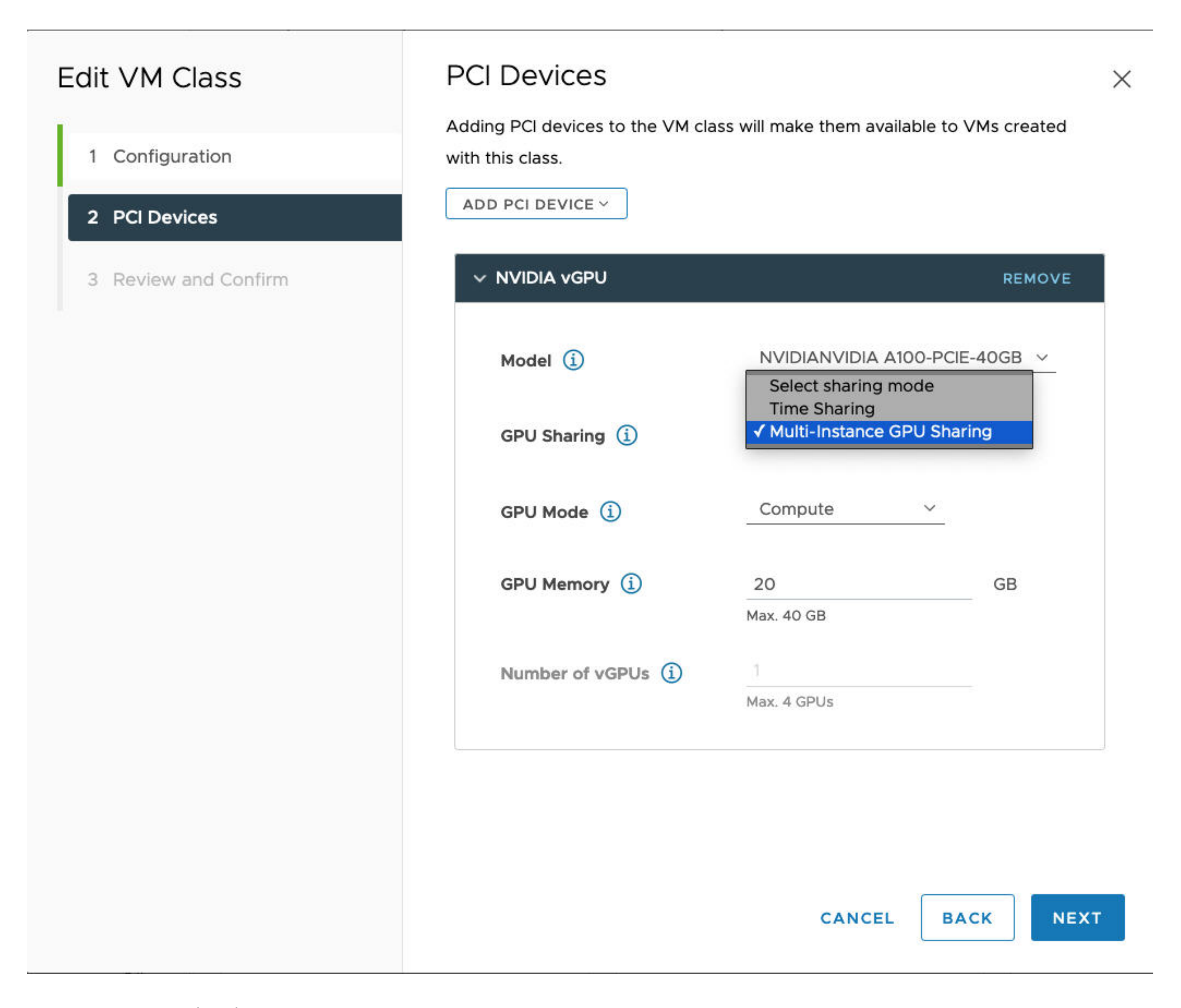
9 Configure el modelo NVIDIA vGPU.

Campo NVIDIA vGPU	Descripción
Modelo	Seleccione el modelo del dispositivo de hardware GPU NVIDIA de los disponibles en el menú **vGPU de NVIDIA > Modelo**. Si el sistema no muestra ningún perfil, ninguno de los hosts del clúster tiene dispositivos PCI compatibles.
Uso compartido de GPU	Este ajuste define cómo se comparte el dispositivo GPU entre máquinas virtuales habilitadas para GPU. Existen dos tipos de implementaciones de vGPU: **Uso compartido de tiempo** y **Uso compartido de GPU de varias instancias**. En el modo de Uso compartido de tiempo, el programador de vGPU indica a la GPU que realice el trabajo para cada máquina virtual habilitada para vGPU en serie durante un período de tiempo con el mejor objetivo de esfuerzo de equilibrar el rendimiento entre las vGPU. El modo MIG permite que varias máquinas virtuales habilitadas para vGPU se ejecuten en paralelo en un solo dispositivo GPU. El modo MIG se basa en una arquitectura de GPU más reciente y solo se admite en dispositivos NVIDIA A100 y A30. Si no ve la opción MIG, el dispositivo PCI que seleccionó no lo admite.
Modo GPU	**Cálculo**
Memoria de GPU	**8 GB**, por ejemplo
Número de vGPU	**1**, por ejemplo

Por ejemplo, este es un perfil de NVIDIA vGPU configurado en el modo Uso compartido de tiempo:



Por ejemplo, aquí se muestra un perfil de NVIDIA vGPU configurado en el modo MIG con un dispositivo GPU compatible:



10 Haga clic en **Siguiente**.

11 Revise y confirme las selecciones que hizo.

12 Haga clic en **Finalizar**.

13 Compruebe que la nueva clase de máquina virtual personalizada esté disponible en la lista de clases de máquinas virtuales.

Paso 8 de administración: Crear y configurar un espacio de nombres de vSphere para el clúster GPU de TKGS

Cree un espacio de nombres de vSphere para cada clúster GPU de TKGS que tenga previsto aprovisionar. Para configurar el espacio de nombres, agregue un usuario de SSO de vSphere con permisos de edición y asocie una directiva de almacenamiento para volúmenes persistentes.

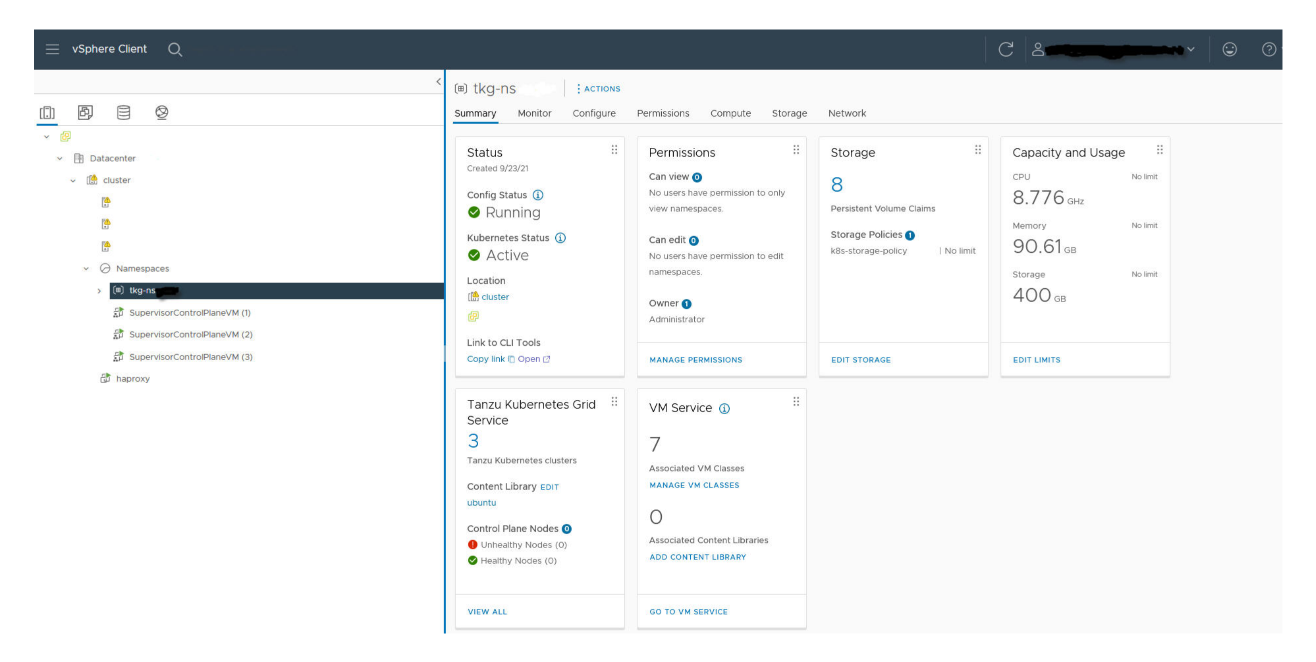
Para ello, vea Creación y configuración de un espacio de nombres de vSphere.

Paso 9 del administrador: Asociar la biblioteca de contenido y la clase de máquina virtual con el espacio de nombres de vSphere

Después de crear y configurar el espacio de nombres de vSphere, asocie la biblioteca de contenido que incluye el archivo OVA de Ubuntu con el espacio de nombres de vSphere, y asocie la clase de máquina virtual personalizada con el perfil de vGPU con el mismo espacio de nombres de vSphere.

Tarea	Descripción
Asocie la biblioteca de contenido con el archivo OVA de Ubuntu para vGPU con el espacio de nombres de vSphere en el que aprovisionará el clúster TKGS.	Consulte Configurar un espacio de nombres de vSphere para las versiones de Tanzu Kubernetes.
Asocie la clase de máquina virtual personalizada con el perfil de vGPU con el espacio de nombres de vSphere en el que aprovisionará el clúster TKGS.	Consulte Asociar una clase de máquina virtual con un espacio de nombres en vSphere with Tanzu.

El siguiente ejemplo muestra un espacio de nombres de vSphere configurado con una biblioteca de contenido asociada y una clase de máquina virtual personalizada para su uso con clústeres de vGPU.



Paso 10 del administrador: comprobar que se pueda acceder al clúster supervisor

La última tarea de administración consiste en comprobar que el clúster supervisor esté aprovisionado y disponible para que lo pueda utilizar el operador del clúster a fin de aprovisionar un clúster TKGS para cargas de trabajo de AI/ML.

1 Descargue e instale las Herramientas de la CLI de Kubernetes para vSphere.

   Consulte Descargar e instalar Herramientas de la CLI de Kubernetes para vSphere.

2 Conéctese al clúster supervisor.

   Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

3 Proporcione al operador de clúster el vínculo con el que puede descargar las Herramientas de la CLI de Kubernetes para vSphere y el nombre del espacio de nombres de vSphere.

Consulte Flujo de trabajo de operadores de clúster para implementar cargas de trabajo de AI/ML en clústeres TKGS.

Flujo de trabajo de operadores de clúster para implementar cargas de trabajo de AI/ML en clústeres TKGS

Para permitir que los desarrolladores implementen cargas de trabajo de AI/ML en clústeres TKGS, como operador de clúster, configure el entorno de Kubernetes para que admita operaciones de NVIDIA vGPU.

Flujo de trabajo de operadores de clúster para implementar cargas de trabajo de AI/ML en clústeres TKGS

Los pasos de alto nivel para implementar cargas de trabajo de AI/ML en clústeres TKGS son los siguientes:

Paso	Acción	Vincular
0	Revise los requisitos del sistema.	Consulte Paso 0 del operador: Revisar los requisitos del sistema.
1	Descargue kubectl y el complemento de vSphere para Kubectl en la estación de trabajo local.	Consulte Paso 1 del operador: Instalar las Herramientas de la CLI de Kubernetes para vSphere en tu estación de trabajo.
2	Utilice kubectl para iniciar sesión en el clúster supervisor, el cual rellena .kube/config con el contexto del nuevo clúster supervisor.	Consulte Paso 2 del operador: Iniciar sesión en el clúster supervisor.
3	Utilice kubectl para cambiar el contexto al espacio de nombres de vSphere.	Consulte Paso 3 del operador: Cambiar el contexto al espacio de nombres de vSphere.
4	Utilice kubectl para enumerar las clases de máquina virtual y comprobar que está incluida la clase habilitada para NVIDIA vGPU.	Consulte Paso 4 del operador: Obtener la clase de máquina virtual personalizada para cargas de trabajo de vGPU.
5	Utilice kubectl para enumerar las versiones de Tanzu Kubernetes disponibles y comprobar que está incluida la imagen de Ubuntu.	Consulte Paso 5 del operador: Obtener la versión de Tanzu Kubernetes de Ubuntu para los nodos de GPU.
6	Diseñe la especificación de YAML para aprovisionar el clúster TKGS habilitado para GPU; especifique la versión de TKR y la clase de máquina virtual.	Consulte Paso 6 del operador: Diseñar el YAML para aprovisionar el clúster TKGS habilitado para vGPU.
7	Aprovisione el clúster TKGS.	Consulte Paso 7 del operador: Aprovisionar el clúster TKGS.
8	Inicie sesión en el clúster y compruebe el aprovisionamiento.	Consulte Paso 8 del operador: Iniciar sesión en el clúster TKGS y comprobar el aprovisionamiento.

Paso	Acción	Vincular
9	Prepárese para instalar el operador de GPU NVAIE. Para ello, cree algunos objetos como requisito previo en el clúster TKGS, incluidos un espacio de nombres, enlaces de funciones, el secreto de imagen y el mapa de configuración de licencia.	Consulte Paso 9 del operador: Prepararse para instalar el operador de GPU NVAIE.
10	Instale el operador de GPU NVAIE en el clúster.	Consulte Paso 10 del operador: Instalar el operador de GPU NVIDIA en el clúster.
11	Implemente cargas de trabajo de AI/ML en el clúster TKGS habilitado para vGPU.	Consulte Paso 11 del operador: Implementar una carga de trabajo de AI/ML.

Paso 0 del operador: Revisar los requisitos del sistema

Consulte los siguientes requisitos del sistema para configurar el entorno de implementación de cargas de trabajo de AI/ML en clústeres TKGS.

Requisito	Descripción
El administrador de vSphere ha configurado el entorno para NVIDIA vGPU	Consulte Flujo de trabajo del administrador de vSphere para implementar cargas de trabajo de AI/ML en clústeres TKGS (vGPU).
OVA de TKR Ubuntu	versión de Tanzu Kubernetes Ubuntu `ob-18691651-tkgs-ova-ubuntu-2004-v1.20.8---vmware.1-tkg.2`
Aprovisionador de clúster TKG	servicio Tanzu Kubernetes Grid Versión de API: `run.tanzu.vmware.com/v1alpha2`
Operador de GPU NVIDIA	Operador de GPU v1.8.0
Contenedor del controlador de GPU NVIDIA	`nvcr.io/nvstating/cnt-ea/driver:470.51-ubuntu20.04`

Paso 1 del operador: Instalar las Herramientas de la CLI de Kubernetes para vSphere en tu estación de trabajo

Descargue e instale las Herramientas de la CLI de Kubernetes para vSphere.

Si utiliza Linux, puede ejecutar el siguiente comando para descargar las herramientas.

```
curl -LOk https://${SC_IP}/wcp/plugin/linux-amd64/vsphere-plugin.zip
unzip vsphere-plugin.zip
mv -v bin/* /usr/local/bin/
```

Para obtener más instrucciones, consulte Descargar e instalar Herramientas de la CLI de Kubernetes para vSphere.

Paso 2 del operador: Iniciar sesión en el clúster supervisor

Utilice el complemento de vSphere para kubectl para autenticarse en clúster supervisor.

```
kubectl vsphere login --server=IP-ADDRESS --vsphere-username USERNAME
```

Paso 3 del operador: Cambiar el contexto al espacio de nombres de vSphere

Con kubectl, cambie el contexto al espacio de nombres de vSphere que creó el administrador de vSphere para el clúster de GPU TKGS.

```
kubectl config get-contexts
```

```
kubectl config use-context TKGS-GPU-CLUSTER-NAMESPACE
```

Paso 4 del operador: Obtener la clase de máquina virtual personalizada para cargas de trabajo de vGPU

Compruebe que la clase de máquina virtual personalizada con el perfil de vGPU que creó el administrador de vSphere esté disponible en el espacio de nombres de vSphere de destino.

```
kubectl get virtualmachineclassbindings
```

Nota La clase de máquina virtual debe estar enlazada al espacio de nombres de vSphere de destino. Si no ve la clase de máquina virtual personalizada para cargas de trabajo de vGPU, consulte con el administrador de vSphere.

Paso 5 del operador: Obtener la versión de Tanzu Kubernetes de Ubuntu para los nodos de GPU

Compruebe que la versión de Tanzu Kubernetes de Ubuntu que se requiere y que sincronizó el administrador de vSphere desde la biblioteca de contenido esté disponible en el espacio de nombres de vSphere.

```
kubectl get tanzukubernetesreleases
```

O bien utilice el acceso directo:

```
kubectl get tkr
```

Paso 6 del operador: Diseñar el YAML para aprovisionar el clúster TKGS habilitado para vGPU

Cree el archivo YAML para el aprovisionamiento de un clúster de Tanzu Kubernetes.

Comience con uno de los siguientes ejemplos. Utilice la información que recopiló entre los resultados de los comandos anteriores para personalizar la especificación del clúster. Consulte la lista completa de parámetros de configuración: API v1alpha2 de TKGS para aprovisionar clústeres de Tanzu Kubernetes

El ejemplo 1 especifica dos grupos de nodos de trabajo.

```
apiVersion: run.tanzu.vmware.com/v1alpha2
kind: TanzuKubernetesCluster
metadata:
   #cluster name
```

```
  name: tkgs-cluster-gpu-a100
  #target vsphere namespace
  namespace: tkgs-gpu-operator
spec:
  topology:
    controlPlane:
      replicas: 3
      #storage class for control plane nodes
      #use `kubectl describe storageclasses`
      #to get available pvcs
      storageClass: vwt-storage-policy
      vmClass: guaranteed-medium
      #TKR NAME for Ubuntu ova supporting GPU
      tkr:
        reference:
          name: 1.20.8---vmware.1-tkg.1
    nodePools:
    - name: nodepool-a100-primary
      replicas: 3
      storageClass: vwt-storage-policy
      #custom VM class for vGPU
      vmClass: class-vgpu-a100
      #TKR NAME for Ubuntu ova supporting GPU
      tkr:
        reference:
          name: 1.20.8---vmware.1-tkg.1
    - name: nodepool-a100-secondary
      replicas: 3
      vmClass: class-vgpu-a100
      storageClass: vwt-storage-policy
      #TKR NAME for Ubuntu ova supporting GPU
      tkr:
        reference:
          name: 1.20.8---vmware.1-tkg.1
  settings:
    storage:
      defaultClass: vwt-storage-policy
    network:
      cni:
       name: antrea
      services:
       cidrBlocks: ["198.51.100.0/12"]
      pods:
       cidrBlocks: ["192.0.2.0/16"]
      serviceDomain: managedcluster.local
```

El ejemplo 2 especifica un volumen independiente en los nodos de trabajo para el tiempo de ejecución en contenedor con una capacidad de 50 GiB. Esta opción se puede configurar. Se recomienda proporcionar un volumen independiente de buen tamaño para las cargas de trabajo de AI/ML basadas en contenedores.

```
apiVersion: run.tanzu.vmware.com/v1alpha2
kind: TanzuKubernetesCluster
metadata:
  name: tkc
  namespace: tkg-ns-auto
spec:
  distribution:
    fullVersion: v1.20.8+vmware.1-tkg.1
  topology:
    controlPlane:
      replicas: 3
      storageClass: vwt-storage-policy
      tkr:
        reference:
          name: v1.20.8---vmware.1-tkg.1
      vmClass: best-effort-medium
    nodePools:
    - name: workers
      replicas: 3
      storageClass: k8s-storage-policy
      tkr:
        reference:
          name: v1.20.8---vmware.1-tkg.1
      vmClass: vmclass-vgpu
      volumes:
      - capacity:
          storage: 50Gi
        mountPath: /var/lib/containerd
        name: containerd
      - capacity:
          storage: 50Gi
        mountPath: /var/lib/kubelet
        name: kubelet
    - name: nodepool-1
      replicas: 1
      storageClass: vwt-storage-policy
      vmClass: best-effort-medium
```

El ejemplo 3 incluye metadatos adicionales del clúster, como una etiqueta.

```
apiVersion: run.tanzu.vmware.com/v1alpha2
kind: TanzuKubernetesCluster
metadata:
  annotations:
  labels:
    run.tanzu.vmware.com/tkr: v1.20.8---vmware.1-tkg.1
  name: tkgs-gpu-direct-rdma
  namespace: tkgs-ns
spec:
```

```
  settings:
    network:
      cni:
        name: antrea
      pods:
        cidrBlocks:
        - 192.168.0.0/16
      serviceDomain: cluster.local
      services:
        cidrBlocks:
        - 10.96.0.0/12
  topology:
    controlPlane:
      replicas: 3
      storageClass: tkgs-storage-policy
      vmClass: guaranteed-medium
      tkr:
        reference:
          name: v1.20.8---vmware.1-tkg.1
    nodePools:
    - name: workers
      replicas: 5
      storageClass: tkgs-storage-policy
      vmClass: claire-gpu-direct-rdma
      volumes:
      - capacity:
          storage: 50Gi
        mountPath: /var/lib/containerd
        name: containerd
      - capacity:
          storage: 50Gi
        mountPath: /var/lib/kubelet
        name: kubelet
      tkr:
        reference:
          name: v1.20.8---vmware.1-tkg.1
```

Paso 7 del operador: Aprovisionar el clúster TKGS

Ejecute el siguiente comando kubectl para aprovisionar el clúster.

```
kubectl apply -f CLUSTER-NAME.yaml
```

Por ejemplo:

```
kubectl apply -f tkgs-gpu-cluster-1.yaml
```

Supervise la implementación de nodos del clúster mediante kubectl.

```
kubectl get tanzukubernetesclusters -n NAMESPACE
```

Paso 8 del operador: Iniciar sesión en el clúster TKGS y comprobar el aprovisionamiento

Con el complemento de vSphere para kubectl, inicie sesión en el clúster TKGS.

```
kubectl vsphere login --server=IP-ADDRESS --vsphere-username USERNAME \
--tanzu-kubernetes-cluster-name CLUSTER-NAME --tanzu-kubernetes-cluster-namespace NAMESPACE-
NAME
```

Con los comandos siguientes, compruebe el clúster:

```
kubectl cluster-info
```

```
kubectl get nodes
```

```
kubectl get namespaces
```

```
kubectl api-resources
```

Paso 9 del operador: Prepararse para instalar el operador de GPU NVAIE

Antes de instalar el operador de GPU con NVIDIA AI Enterprise, complete las siguientes tareas para el clúster TKGS que aprovisionó. Para obtener más instrucciones, consulte Tareas obligatorias previas en la documentación de NVAIE.

Nota Si utiliza el servidor de licencias delegado (DLS) de NVIDIA, consulte el siguiente tema para obtener instrucciones: Anexo de operadores de clúster para implementar cargas de trabajo de AI/ML en clústeres TKGS (DLS)

1 Cree el espacio de nombres de Kubernetes `gpu-operator-resources`. Como práctica recomendada, implemente siempre todo lo que haya en este espacio de nombres.

   ```
   kubectl create ns gpu-operator-resources
   ```

2 Cree enlaces de funciones.

   Los clústeres de Tanzu Kubernetes tienen habilitada la directiva de seguridad de pods.

   Cree `rolebidings.yaml`.

   ```
   apiVersion: rbac.authorization.k8s.io/v1
   kind: RoleBinding
   metadata:
     name: psp:vmware-system-privileged:default
     namespace: default
   roleRef:
     apiGroup: rbac.authorization.k8s.io
     kind: ClusterRole
     name: psp:vmware-system-privileged
   subjects:
   - apiGroup: rbac.authorization.k8s.io
   ```

```
  kind: Group
  name: system:nodes
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:serviceaccounts
```

Aplique el enlace de función.

```
kubectl apply -f rolebindings.yaml
```

Cree `post-rolebindings.yaml`.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: psp:vmware-system-privileged:gpu-operator-resources
  namespace: gpu-operator-resources
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: psp:vmware-system-privileged
subjects:
- kind: Group
  apiGroup: rbac.authorization.k8s.io
  name: system:serviceaccounts
```

Aplique el enlace de función:

```
kubectl apply -f post-rolebindings.yaml
```

3 Cree un secreto de imagen con credenciales de NGC que Docker pueda utilizar para extraer imágenes de contenedor del catálogo de NVIDIA GPU Cloud.

```
kubectl create secret docker-registry registry-secret \
     --docker-server=server-name --docker-username='$oauthtoken' \
     --docker-password=<place_holder> \
     --docker-email=email-name -n gpu-operator-resources
```

4 Cree un mapa de configuración para el servidor de licencias de NVIDIA.

```
kubectl create configmap licensing-config -n gpu-operator-resources --from-file=gridd.conf
```

`gridd.conf` hace referencia a la dirección del servidor de licencias de NVIDIA; por ejemplo:

```

# Description: Set License Server Address
# Data type: string
# Format:  "<address>"
ServerAddress=<place_holder>
```

Paso 10 del operador: Instalar el operador de GPU NVIDIA en el clúster

Instale la versión 1.8.0 del operador de GPU NVAIE en el clúster TKGS. Para ver más instrucciones, consulte la documentación del operador de GPU.

Nota Si utiliza el servidor de licencias delegado (DLS) de NVIDIA, consulte el siguiente tema para obtener instrucciones: Anexo de operadores de clúster para implementar cargas de trabajo de AI/ML en clústeres TKGS (DLS)

1 Para instalar Helm, consulte la documentación de Helm.

2 Agregue el repositorio de Helm `gpu-operator`.

```
helm repo add nvidia https://nvidia.github.io/gpu-operator
```

3 Instale el operador de GPU NVAIE con el siguiente comando.

Cuando sea necesario, sustituya los valores de variable de entorno por los que coincidan con su entorno.

```
export PRIVATE_REGISTRY="private/registry/path"
export OS_TAG=ubuntu20.04
export VERSION=460.73.01
export VGPU_DRIVER_VERSION=460.73.01-grid
export NGC_API_KEY=ZmJjMHZya...LWExNTRi
export REGISTRY_SECRET_NAME=registry-secret

helm install nvidia/gpu-operator \
   --set driver.repository=$PRIVATE_REGISTRY \
   --set driver.version=$VERSION \
   --set driver.imagePullSecrets={$REGISTRY_SECRET_NAME} \
   --set operator.defaultRuntime=containerd \
   --set driver.licensingConfig.configMapName=licensing-config
```

Paso 11 del operador: Implementar una carga de trabajo de AI/ML

El catálogo de NVIDIA GPU Cloud ofrece varias imágenes de contenedor que se encuentran disponibles para ejecutar cargas de trabajo de AI/ML en los clústeres de Tanzu Kubernetes habilitados para vGPU. Para obtener más información sobre las imágenes disponibles, consulte la documentación de NGC.

Anexo del administrador de vSphere para implementar cargas de trabajo de AI/ML en clústeres TKGS (vGPU e Instancia dinámica de DirectPath I/O)

Consulte este tema delta si va a configurar TKGS para admitir cargas de trabajo de AI/ML mediante vGPU e Instancia dinámica de DirectPath I/O.

Ajustes del flujo de trabajo del administrador de vSphere para vGPU con Instancia dinámica de DirectPath I/O

Para utilizar vGPU e Instancia dinámica de DirectPath I/O, siga el mismo Flujo de trabajo del administrador de vSphere para implementar cargas de trabajo de AI/ML en clústeres TKGS (vGPU) con los siguientes cambios.

Paso 2 del administrador: Habilitar el acceso directo para el dispositivo PCI

Para utilizar vGPU e Instancia dinámica de DirectPath I/O, configure cada host ESXi para vGPU que se describe aquí: Paso 2 del administrador: Configurar cada host ESXi para operaciones de vGPU.

Además, configure el dispositivo GPU de la siguiente manera.

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Seleccione el host ESXi de destino en el clúster de vCenter.

3 Seleccione **Configurar > Hardware > Dispositivos PCI**.

4 Seleccione la pestaña **Todos los dispositivos PCI**.

5 Seleccione el dispositivo acelerador de NVIDIA GPU de destino.

6 Haga clic en **Alternar acceso directo**.

7 Haga clic con el botón secundario en el host ESXi y póngalo en el modo de mantenimiento.

8 Reinicie el host.

9 Cuando el host vuelva a ejecutarse, salga del modo de mantenimiento.

Paso 7 de administración: Crear una clase de máquina virtual personalizada con una vGPU y una Instancia dinámica de DirectPath I/O

Para utilizar vGPU e Instancia dinámica de DirectPath I/O, configure una clase de máquina virtual personalizada con un perfil **NVIDIA vGPU** como se describe aquí: Paso 7 del administrador: Crear una clase de máquina virtual personalizada con el perfil de vGPU.

A continuación, a esta clase de máquina virtual se agrega una segunda configuración de dispositivo PCI con **Instancia dinámica de DirectPath I/O** especificada y el dispositivo PCI compatible seleccionado. Cuando se crea una instancia de una clase de máquina virtual de este tipo, vSphere Distributed Resource Scheduler (DRS) determina la colocación de la máquina virtual.

Consulte las siguientes instrucciones para crear una clase de máquina virtual personalizada compatible con vGPU e Instancia dinámica de DirectPath I/O. Para obtener más instrucciones, consulte Agregar dispositivos PCI a una clase de máquina virtual en vSphere with Tanzu.

1 Inicie sesión en vCenter Server con vSphere Client.

2 Seleccione **Administración de cargas de trabajo**.

3 Seleccione **Servicios**

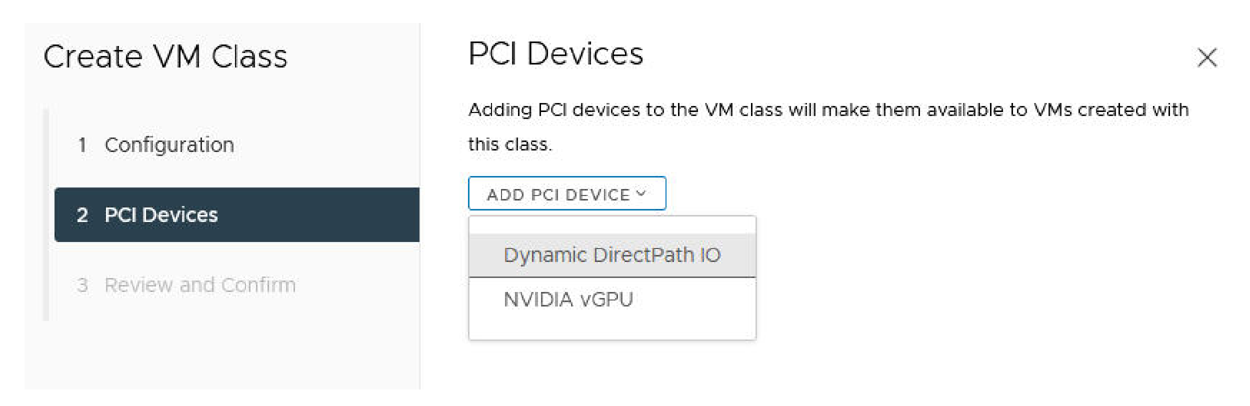
4 Seleccione **Clases de VM**.

5 Edite la clase de máquina virtual personalizada que ya está configurada con un perfil de **vGPU de NVIDIA**.

6 Seleccione la pestaña **Dispositivos PCI**.

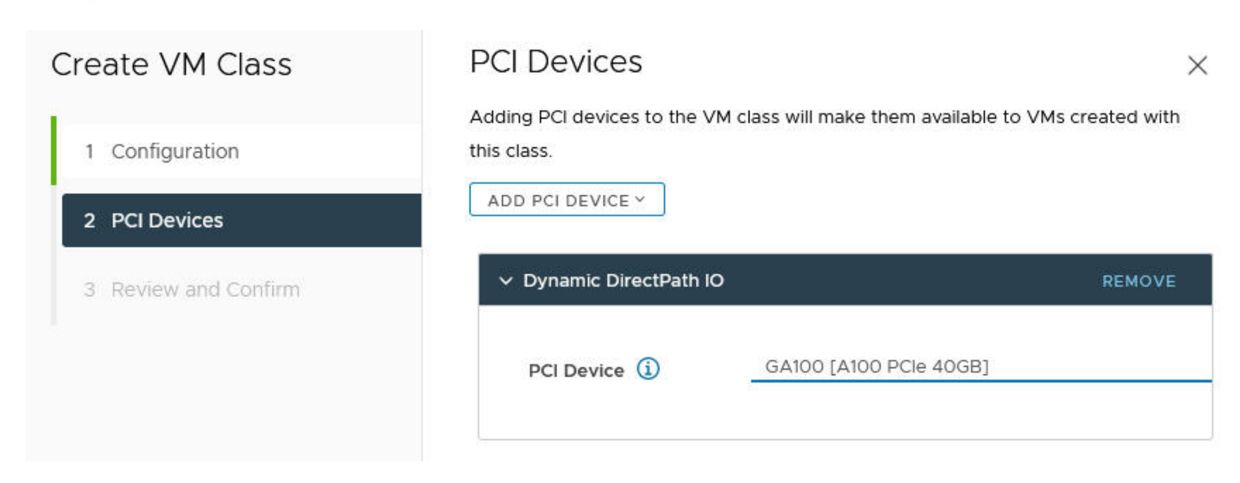
7 Haga clic en **Agregar dispositivo PCI**.

8 Seleccione la opción **Instancia dinámica de DirectPath I/O**.



9 Seleccione el **Dispositivo PCI**.

Por ejemplo:



10 Haga clic en **Siguiente**.

11 Revise y confirme las selecciones que hizo.

12 Haga clic en **Finalizar**.

13 Compruebe que la nueva clase de máquina virtual personalizada esté disponible en la lista de clases de máquinas virtuales.

Anexo de operadores de clúster para implementar cargas de trabajo de AI/ML en clústeres TKGS (DLS)

Consulte este tema delta si utiliza el servidor de licencias delegado (DLS) de NVIDIA para su cuenta de NVIDIA AI Enterprise.

Anexo de operadores de clúster para implementar cargas de trabajo de AI/ML en clústeres TKGS

NVIDIA proporciona un nuevo sistema de servidor de licencias NVIDIA (NLS) denominado DLS, que significa servidor delegado de licencias (DLS, Delegated Licensing Server). Para obtener más información, consulte la documentación de NVIDIA.

Si utiliza DLS para su cuenta de NVAIE, los pasos para preparar e implementar el operador de GPU NVAIE son diferentes de los que se describen aquí: Flujo de trabajo de operadores de clúster para implementar cargas de trabajo de AI/ML en clústeres TKGS. En concreto, los pasos 9 y 10 se modifican de la siguiente manera.

Paso 9 del operador: Prepararse para instalar el operador de GPU NVAIE

Complete los siguientes pasos para preparar la instalación del operador de GPU mediante un DLS.

1 Cree un secreto.

```
kubectl create secret docker-registry registry-secret \
  --docker-server=<users private NGC registry name>
  --docker-username='$oauthtoken' \
  --docker-password=ZmJj…………Ri \
  --docker-email=<user-email-address> -n gpu-operator-resources
```

Nota La contraseña es la clave de API de usuario que se creó previamente en el portal de NVIDIA GPU Cloud (NGC).

2 Obtenga un token de cliente del servidor DLS.

Un usuario que desee utilizar una licencia de vGPU tendrá que obtener un token de ese servidor de licencias DLS denominado "token de cliente". El mecanismo para hacerlo se encuentra en la documentación de NVIDIA.

3 Cree un objeto ConfigMap en el clúster TKGS mediante el token de cliente.

Coloque el archivo del token de cliente en un archivo en `<ruta>/client_configuration_token.tok`.

A continuación, ejecute el siguiente comando:

```
kubectl delete configmap licensing-config -n gpu-operator-resources; > gridd.conf
kubectl create configmap licensing-config \
  -n gpu-operator-resources --from-file=./gridd.conf --from-file=./
client_configuration_token.tok
```

Nota El archivo grid.conf que utiliza el servidor DLS está vacío. Sin embargo, ambos parámetros "--from-file" son obligatorios.

Paso 10 del operador: Instalar el operador de GPU NVAIE

Complete los siguientes pasos para instalar el operador de GPU NVAIE mediante un servidor DLS. Para ver más instrucciones, consulte la documentación del operador de GPU.

1 Instale el operador de GPU NVAIE en el clúster TKGS.

- Para instalar Helm, consulte la documentación de Helm.
- Agregue el repositorio de Helm `gpu-operator`.

```
helm repo add nvidia https://nvidia.github.io/gpu-operator
```

- Instale el operador de GPU mediante Helm.

```
export PRIVATE_REGISTRY="<user's private registry name>"
export OS_TAG=ubuntu20.04
export VERSION=470.63.01
export VGPU_DRIVER_VERSION=470.63.01-grid
export NGC_API_KEY=Zm…………Ri  <- The user's NGC AP Key
export REGISTRY_SECRET_NAME=registry-secret

helm show chart .
kubectl delete crd clusterpolicies.nvidia.com
helm install gpu-operator . -n gpu-operator-resources \
  --set psp.enabled=true \
  --set driver.licensingConfig.configMapName=licensing-config \
  --set operator.defaultRuntime=containerd \
  --set driver.imagePullSecrets={$REGISTRY_SECRET_NAME} \
  --set driver.version=$VERSION \
  --set driver.repository=$PRIVATE_REGISTRY \
  --set driver.licensingConfig.nlsEnabled=true
```

2 Compruebe que el servidor DLS ha funcionado.

Desde un pod DaemonSet del controlador de NVIDIA que implementó el operador de GPU, ejecute el comando `nvidia-smi` para comprobar que el servidor DLS funciona.

En primer lugar, ejecute el siguiente comando para acceder al pod y activar una sesión de shell:

```
kubectl exec -it nvidia-driver-daemonset-cvxx6 nvidia-driver-ctr -n gpu-operator-resources
- bash
```

Ahora puede ejecutar el comando para comprobar la configuración del servidor DLS.

```
nvidia-smi
```

Si DLS está configurado correctamente, este comando debe devolver "Con licencia" en los resultados.

Usar un registro de contenedores para cargas de trabajo de vSphere with Tanzu

15

Los registros de contenedor proporcionan a los operadores de Kubernetes un repositorio adecuado para almacenar y compartir imágenes de contenedor. vSphere with Tanzu incluye un registro de Harbor integrado que puede habilitar en el clúster supervisor. Además, puede utilizar un registro de contenedor privado externo con clústeres de Tanzu Kubernetes.

Puede habilitar la instancia integrada de registro de Harbor en el clúster supervisor para que sirva como registro de contenedor privado para la implementación de cargas de trabajo de clústeres de pods de vSphere y Tanzu Kubernetes. Proporcione la URL del registro a los desarrolladores que pueden utilizar el complemento auxiliar de credenciales de vSphere Docker para acceder de forma segura al registro e insertar y extraer imágenes de contenedor.

Nota El registro de Harbor integrado requiere que el clúster supervisor esté configurado para usar redes de NSX-T.

Como alternativa al registro de Harbor integrado, o además de este, puede configurar los clústeres de Tanzu Kubernetes para que usen un registro de contenedor privado externo.

Este capítulo incluye los siguientes temas:

- Habilitar el registro de Harbor integrado en el clúster supervisor
- Iniciar sesión en la consola del registro de Harbor integrado
- Descargar e instalar el certificado de registro de Harbor integrado
- Configurar un cliente de Docker con un certificado de registro de Harbor integrado
- Instalar el complemento auxiliar de credenciales de vSphere Docker y conectarse con el registro
- Insertar imágenes en el registro de Harbor integrado
- Purgar imágenes del registro de Harbor integrado
- Utilizar el registro de Harbor integrado con clústeres de Tanzu Kubernetes
- Usar un registro de contenedor externo con clústeres de Tanzu Kubernetes

Habilitar el registro de Harbor integrado en el clúster supervisor

Como administrador de vSphere, puede habilitar el registro de Harbor que está integrado con vSphere with Tanzu. Puede insertar y extraer imágenes del contenedor desde el registro, así como implementar contenedores mediante dichas imágenes.

Una vez que se habilite el registro de Harbor, cada espacio de nombres del clúster supervisor tiene un proyecto que coincide con el mismo nombre que el registro de la imagen privada. Todos los usuarios o grupos que tengan permisos de edición o visualización en un espacio de nombres se convierten en miembros con la función correspondiente en el proyecto que coincide con el mismo nombre en el registro de imágenes privadas. El ciclo de vida de los proyectos y los miembros del registro de imágenes privadas se administra automáticamente y está vinculado al ciclo de vida de los permisos de los espacios de nombres y usuarios o grupos en espacios de nombres.

Requisitos previos

Para habilitar el registro de Harbor integrado, debe haber habilitado **Administración de cargas de trabajo** e implementado un clúster supervisor. Además, debe crear una directiva de almacenamiento para la colocación de imágenes de contenedor. Esta directiva de almacenamiento se utiliza para aprovisionar volúmenes persistentes que se utilizarán como almacén de respaldo para las imágenes de contenedor en el registro.

Nota Para usar el registro de Harbor integrado, debe implementar el clúster supervisor con NSX-T Data Center como la solución de redes. Consulte Configurar NSX-T Data Center para vSphere with Tanzu.

Procedimiento

1. En vSphere Client, desplácese hasta el clúster de vCenter donde está habilitada **Administración de cargas de trabajo**.
2. Seleccione **Configurar**.
3. Seleccione **Clúster supervisor**.
4. Seleccione **Registro de imágenes**.
5. Haga clic en **Habilitar puerto**.
6. Seleccione la **Directiva de almacenamiento** para la colocación de imágenes de contenedor.
7. Haga clic en **Aceptar** para completar el proceso.

Resultados

Un registro de imagen privada se habilita después de unos minutos. Se crea un espacio de nombres especial para esa instancia del registro de la imagen privada. No puede realizar ninguna operación en ese espacio de nombres, ya que es de solo lectura para los usuarios de vSphere.

Pasos siguientes

Iniciar sesión en la consola del registro de Harbor integrado.

Iniciar sesión en la consola del registro de Harbor integrado

Use la consola de administración del registro de Harbor integrado para administrar y operar el registro privado.

Como administrador de vSphere, puede utilizar la consola de administración del registro de Harbor integrado para crear y administrar proyectos, ver los registros y explorar la API de Harbor.

Requisitos previos

Habilitar el registro de Harbor integrado en el clúster supervisor

Procedimiento

1 En vSphere Client, desplácese hasta el clúster de vCenter donde está habilitada **Administración de cargas de trabajo**.

2 Seleccione **Configurar**.

3 En **Espacios de nombres**, seleccione **Registro de imágenes**.

4 Haga clic en el **Enlace a la interfaz de usuario de Harbor**.

   Se mostrará la página de inicio de sesión de la consola del registro de Harbor integrado.

5 Inicie sesión con sus credenciales de administrador de vSphere.

Descargar e instalar el certificado de registro de Harbor integrado

Descargue el certificado de CA raíz del registro de Harbor integrado a fin de usarlo para conectar clientes al registro.

Para iniciar sesión en el registro de Harbor integrado mediante un cliente de Docker, debe instalar el certificado de CA raíz en ese cliente.

Requisitos previos

En esta tarea se supone que instaló y configuró Docker en un equipo host cliente. Además, el registro de Harbor integrado debe estar habilitado. Consulte Habilitar el registro de Harbor integrado en el clúster supervisor.

Procedimiento

1 Descargue el certificado del registro de Harbor integrado. Existen dos formas de hacerlo.

- Mediante la interfaz de la consola del registro de Harbor integrado.
  - Inicie sesión en la consola del registro de Harbor integrado mediante la dirección URL. Consulte Iniciar sesión en la consola del registro de Harbor integrado.
  - Haga clic en el vínculo del proyecto en la página **Proyectos > Nombre de proyecto**.
  - Seleccione la pestaña **Repositorios**.
  - Haga clic en **Certificado del registro**.
  - Guarde el archivo de certificado `ca.crt` en su máquina local.
- Mediante vSphere Client.
  - Seleccione el clúster de vCenter en el que se habilita **Administración de cargas de trabajo** y el registro de Harbor integrado.
  - Seleccione **Configurar > Espacios de nombres > Registro de imágenes**.
  - En el campo **Certificado raíz**, haga clic en el vínculo **Descargar certificado raíz SSL**.
  - Guarde el archivo `root-certificate.txt` en su máquina local.
  - Cambie el nombre del archivo a `ca.crt`.

2 Copie el archivo `ca.crt` del registro de Harbor integrado que descargó en el directorio correspondiente de un host en el que esté instalado Docker. La ubicación predeterminada del certificado es diferente según el tipo de sistema operativo que ejecute el cliente de Docker.

- Linux

```
/etc/docker/certs.d/ca.crt
```

- Mac OS

```
security add-trusted-cert -d -r trustRoot -k ~/Library/Keychains/login.keychain ca.crt
```

Nota Si no instala el archivo `ca.crt` en la ubicación predeterminada, puede transferir la marca de `--tlscacert /path/to/ca.crt` cuando inicie sesión mediante el complemento auxiliar de credenciales de vSphere Docker.

3 Una vez completada la importación, reinicie el daemon de Docker.

- Linux

```
sudo systemctl restart docker.service
```

- Mac

  Utilice la opción de menú del escritorio de Docker **Reiniciar Docker** o el método abreviado de teclado `command R`.

Pasos siguientes

Instalar el complemento auxiliar de credenciales de vSphere Docker y conectarse con el registro

Configurar un cliente de Docker con un certificado de registro de Harbor integrado

Para trabajar con imágenes de contenedor en el registro de Harbor integrado mediante Docker, debe agregar el certificado de registro en el cliente de Docker. El certificado se utiliza para autenticarse en Docker durante el inicio de sesión.

Configure su cliente de Docker para que interactúe con el registro de Harbor integrado. Esta tarea es necesaria para preparar el complemento auxiliar de credenciales de Docker que vSphere proporciona para conectarse e interactuar con el registro de Harbor integrado.

Requisitos previos

En esta tarea se supone que el registro de Harbor integrado está habilitado y puede iniciar sesión:

- Habilitar el registro de Harbor integrado en el clúster supervisor
- Iniciar sesión en la consola del registro de Harbor integrado

Además, en las instrucciones se supone que está utilizando un host Linux (Ubuntu) en el que está instalado el daemon de Docker. Para comprobar que Docker esté instalado y pueda extraer imágenes de Docker Hub, ejecute el siguiente comando:

```
docker run hello-world
```

Resultado esperado:

```
Hello from Docker!
This message shows that your installation appears to be working correctly.
```

Nota Estas instrucciones se comprueban mediante Ubuntu 20.04 y Docker 19.03.

Procedimiento

1 Descargue el certificado del registro de Harbor integrado `root-certificate.txt`. Consulte Descargar e instalar el certificado de registro de Harbor integrado.

2 Cambie el nombre del certificado a `ca.crt`.

3 Copie de forma segura el archivo `ca.crt` en el host de Docker.

4 En el host de Docker, cree una ruta de directorio para el registro privado utilizando la dirección IP de Harbor.

   ```
   /etc/docker/certs.d/IP-address-of-harbor/
   ```

Por ejemplo:

```
mkdir /etc/docker/certs.d/10.179.145.77
```

5 Mueva `ca.crt` a este directorio.

Por ejemplo:

```
 mv ca.crt /etc/docker/certs.d/10.179.145.77/ca.crt
```

6 Reinicie el daemon de Docker.

```
sudo systemctl restart docker.service
```

7 Inicie sesión en el registro de Harbor integrado mediante su cliente de Docker.

```
docker login https://10.179.145.77
```

Debería ver el siguiente mensaje:

```
WARNING! Your password will be stored unencrypted in /home/ubuntu/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store

Login Succeeded
```

Pasos siguientes

Como se indica en el mensaje, por motivos de seguridad, descargue e instale el complemento auxiliar de credenciales de vSphere Docker. Consulte Instalar el complemento auxiliar de credenciales de vSphere Docker y conectarse con el registro.

Instalar el complemento auxiliar de credenciales de vSphere Docker y conectarse con el registro

Utilice la CLI del complemento auxiliar de credenciales de vSphere Docker para insertar imágenes de contenedor de forma segura en el registro de Harbor integrado y exportarlas desde él.

La página de descargas Herramientas de la CLI de Kubernetes incluye un vínculo para descargar el complemento auxiliar de credenciales de vSphere Docker. Utilice el complemento auxiliar de credenciales de vSphere Docker para conectar de forma segura el cliente de Docker al registro de Harbor integrado.

Requisitos previos

- Habilitar el registro de Harbor integrado en el clúster supervisor
-
- Obtenga de su administrador de vSphere el vínculo de la página de descargas de Herramientas de la CLI de Kubernetes para vSphere.

- De forma alternativa, si tiene acceso a la instancia de vCenter Server, obtenga el vínculo de la siguiente manera:
  - Inicie sesión en vCenter Server mediante vSphere Client.
  - Desplácese hasta **vSphere clúster > Espacios de nombres** y seleccione el espacio de nombres de vSphere en el que está trabajando.
  - Seleccione la pestaña **Resumen** y localice el mosaico de **Estado**.
  - Seleccione **Abrir** debajo del encabezado **Vínculo a herramientas de CLI** para abrir la página de descargas. O bien, puede **Copiar** el vínculo.
- Configure un cliente de Docker. Consulte Configurar un cliente de Docker con un certificado de registro de Harbor integrado.

Procedimiento

1 Con un navegador, vaya a la URL de descarga de **Herramientas de la CLI de Kubernetes** correspondiente a su entorno.

2 Desplácese hacia abajo hasta la sección complemento auxiliar de credenciales de vSphere Docker.

3 Seleccione el sistema operativo.

4 Descargue el archivo `vsphere-docker-credential-helper.zip`.

5 Extraiga el contenido del archivo ZIP en un directorio de trabajo.

   El archivo ejecutable binario `docker-credential-vsphere` está disponible.

6 Copie el archivo binario `docker-credential-vsphere` en el host del cliente de Docker.

7 Agregue la ubicación del archivo binario a la variable PATH del sistema.

   Por ejemplo, en Linux:

```
mv docker-credential-vsphere /usr/local/bin/docker-credential-vsphere
```

8 Compruebe la instalación del complemento auxiliar de credenciales de vSphere Docker. Para ello, ejecute el comando `docker-credential-vsphere` en un shell o una sesión de terminal.

   Verá el mensaje de aviso y la lista de opciones de línea de comandos para la CLI.

```

vSphere login manager is responsible for vSphere authentication.
It allows vSphere users to securely login and logout to access Harbor images.

Usage:
  docker-credential-vsphere [command]

Available Commands:
  help        Help about any command
  login       Login into specific harbor server and get authentication
  logout      Logout from Harbor server and erase user token
```

```
Flags:
  -h, --help   help for docker-credential-vsphere

Use "docker-credential-vsphere [command] --help" for more information about a command.
```

9 Inicie sesión en el registro de Harbor integrado.

En primer lugar, compruebe el uso:

```
docker-credential-vsphere login -help
Usage:
  docker-credential-vsphere login [harbor-registry] [flags]

Flags:
  -h, --help               help for login
  -s, --service string     credential store service
      --tlscacert string   location to CA certificate (default "/etc/docker/certs.d/*.crt")
  -u, --user string        vSphere username and password
```

A continuación, inicie sesión con el siguiente comando:

```
docker-credential-vsphere login <container-registry-IP>
```

Se obtiene el token de autenticación y se guarda. En ese momento se inicia la sesión.

```
docker-credential-vsphere login 10.179.145.77
Username: administrator@vsphere.local
Password: INFO[0017] Fetched username and password
INFO[0017] Fetched auth token
INFO[0017] Saved auth token
```

10 Cierre la sesión del registro de Harbor integrado.

```
docker-credential-vsphere logout 10.179.145.77
```

Pasos siguientes

Insertar imágenes en el registro de Harbor integrado .

Insertar imágenes en el registro de Harbor integrado

Puede insertar imágenes del Docker en un proyecto en el registro de Harbor integrado. Los proyectos del registro de Harbor integrado se corresponden con los espacios de nombres de vSphere en un clúster supervisor.

Requisitos previos

Se supone que se completan las siguientes tareas:

- Habilitar el registro de Harbor integrado en el clúster supervisor

- Instalar el complemento auxiliar de credenciales de vSphere Docker y conectarse con el registro

Además, obtenga la cuenta de usuario para la que tenga permisos de escritura en el espacio de nombres que se corresponde con el proyecto en el registro de Harbor donde desea insertar las imágenes.

Por último, necesita una imagen local que pueda insertar en el registro. El siguiente comando extrae la imagen hello-world de Docker Hub. Necesitará una cuenta para poder extraer la imagen.

```
docker run hello-world
```

Resultado esperado:

```
Hello from Docker!
This message shows that your installation appears to be working correctly.
```

Compruebe la imagen mediante el comando `docker images`.

```

docker images
REPOSITORY     TAG                 IMAGE ID           CREATED            SIZE
hello-world    latest              bf756fb1ae65       10 months ago      13.3kB
```

Procedimiento

1 Inicie sesión en registro de Harbor con la aplicación auxiliar de credenciales de Docker de vSphere.

```
docker-credential-vsphere login <container-registry-IP> --user username@domain.com
```

Nota Si bien se puede proporcionar el `--user` *`nombre de usuario`* para el inicio de sesión, debe utilizar la sintaxis UserPrincipalName (UPN) (`--user` *`username@domain.com`*) si desea iniciar sesión y utilizar los comandos `docker push`.

2 Etiquete la imagen que desea insertar en el proyecto en registro de Harbor con el mismo nombre que el espacio de nombres, donde desea utilizarla:

```
docker tag <image-name>[:TAG] <container-registry-IP>/<project-name>/<image-name>[:TAG]
```

Por ejemplo:

```

docker tag hello-world:latest 10.179.145.77/tkgs-cluster-ns/hello-world:latest
```

```

docker images
REPOSITORY                                              TAG                IMAGE ID
CREATED             SIZE
```

```
10.179.145.77/tkgs-cluster-ns/hello-world     latest              bf756fb1ae65        10
months ago       13.3kB
hello-world                                   latest              bf756fb1ae65        10
months ago       13.3kB
```

3 Para insertar una imagen en un proyecto en Harbor, ejecute el siguiente comando:

Sintaxis:

```
docker push <container-registry-IP>/<namespace-name>/<image_name>
```

Por ejemplo:

```
docker push 10.179.145.77/tkgs-cluster-ns/hello-world:latest
```

Resultado esperado.

```

The push refers to repository [10.179.145.77/tkgs-cluster-ns/hello-world]
9c27e219663c: Pushed
latest: digest: sha256:90659bf80b44ce6be8234e6ff90a1ac34acbeb826903b02cfa0da11c82cbc042
size: 525
```

4 Compruebe que la imagen esté ahora disponible en el registro de Harbor integrado.

- Iniciar sesión en la consola del registro de Harbor integrado
- Haga clic en el vínculo del proyecto en **Proyectos > Nombre de proyecto**.
- Seleccione la pestaña **Repositorios**.
- Debería ver que está la imagen que ha insertado en el registro, con el formato `namespace/image-name`, como `tkgs-cluster-ns/hello-world`.
- Seleccione esta imagen y verá la etiqueta `latest` y otros metadatos.

5 Vuelva a la pestaña **Repositorios**.

6 Seleccione el menú desplegable **Comando de Docker para insertar imágenes**. Se le proporcionarán los comandos para etiquetar e insertar imágenes en este repositorio.

Ejemplo

A continuación se muestra otro ejemplo de inserción de imagen en el registro de Harbor integrado:

```
docker tag busybox:latest <container-registry-IP>/<namespace-name>/busybox:latest
docker push <container-registry-IP>/busybox/busybox:latest
```

Pasos siguientes

Implemente pods de vSphere mediante imágenes del registro de Harbor. Consulte Implementar una aplicación en un pod de vSphere mediante el registro de Harbor integrado.

Purgar imágenes del registro de Harbor integrado

Como administrador de vSphere, puede purgar las imágenes de un proyecto del registro de imágenes privado si lo solicitan los ingenieros de desarrollo y operaciones. Al depurar imágenes del registro de imágenes privado, se eliminan todas las referencias a las imágenes realizadas por los pods, pero no se eliminan las imágenes del registro de imágenes.

En caso de que los ingenieros de desarrollo y operaciones informen que hay demasiadas imágenes almacenadas para un proyecto, como administrador de vSphere puede purgar las imágenes de ese proyecto en el registro de imágenes privado. Al purgar las imágenes de un proyecto, se eliminan todas las referencias a estas imágenes, pero no se eliminan del almacén de datos de vSphere. Cada sábado a las 2 a. m., el servicio de recopilador de elementos no utilizados elimina las imágenes de todo el registro de imágenes privado a las que las aplicaciones no hacen referencia.

Procedimiento

1 En el vSphere Client, navegue al espacio de nombres.

2 Seleccione **Configurar** y **General**.

3 Junto a **Registro integrado**, haga clic en **Purgar**.

Utilizar el registro de Harbor integrado con clústeres de Tanzu Kubernetes

Puede utilizar el registro de Harbor integrado para que actúe como registro de contenedor privado de las imágenes que implemente en los clústeres de Tanzu Kubernetes que aprovisiona servicio Tanzu Kubernetes Grid.

vSphere with Tanzu incrusta una instancia del registro de Harbor que puede habilitar en el clúster supervisor y utilizar para implementar cargas de trabajo basadas en contenedores en clústeres de Tanzu Kubernetes.

Una vez que el registro de Harbor integrado esté habilitado en el clúster supervisor, servicio Tanzu Kubernetes Grid instalará en los nodos del clúster de Tanzu Kubernetes el certificado de CA raíz para la instancia del registro. Este certificado se instala en los clústeres nuevos y en los clústeres existentes (a través de un bucle de reconciliación). A partir de ese momento, podrá ejecutar imágenes en el clúster especificando el registro privado en el YAML de carga de trabajo.

Flujo de trabajo

Utilice el siguiente flujo de trabajo para acceder de forma segura al registro privado desde los nodos del clúster de Tanzu Kubernetes y extraer imágenes del contenedor.

Paso	Acción	Instrucciones
0	Revise el flujo de trabajo para usar el registro de Harbor integrado con clústeres de Tanzu Kubernetes.	Consulte Capítulo 15 Usar un registro de contenedores para cargas de trabajo de vSphere with Tanzu.
1	Habilite el registro de Harbor integrado en el clúster supervisor.	Consulte Habilitar el registro de Harbor integrado en el clúster supervisor.
2	Configure kubeconfig para cada clúster con el secreto del servicio de registro.	Consulte las instrucciones a continuación: configure un clúster de Tanzu Kubernetes con el secreto de extracción de imágenes del registro de Harbor integrado.
3	Configure el YAML de carga de trabajo para especificar el registro de contenedor privado.	Consulte las instrucciones a continuación: configure un clúster de Tanzu Kubernetes con el secreto de extracción de imágenes del registro de Harbor integrado.
4	Para insertar imágenes en el registro de Harbor integrado, configure un cliente de Docker e instale el complemento auxiliar de credenciales de vSphere Docker.	Consulte Configurar un cliente de Docker con un certificado de registro de Harbor integrado y Insertar imágenes en el registro de Harbor integrado .

Configurar un clúster de Tanzu Kubernetes con el secreto de extracción de imágenes del registro de Harbor integrado

Configure kubeconfig con el secreto de extracción de imágenes para conectar un clúster de Tanzu Kubernetes a un registro de contenedor privado, ya sea el registro de Harbor integrado o un registro privado externo.

1 Conéctese al clúster supervisor. Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

2 Cambie el contexto al espacio de nombres de vSphere donde se aprovisiona el clúster de Tanzu Kubernetes de destino.

```
kubectl config use-context tkgs-cluster-ns
```

3 Obtenga el secreto de extracción de imágenes para el espacio de nombres de vSphere y guárdelo en un archivo.

```
kubectl get secret -n <vsphere-namespace> <vsphere-namespace>-default-image-pull-secret -o
yaml > <path>/image-pull-secret.yaml
```

Por ejemplo:

```
kubectl get secret -n tkgs-cluster-ns tkgs-cluster-ns-default-image-pull-secret -o yaml >
tanzu/image-pull-secret.yaml
```

4 Abra `image-pull-secret.yaml` con un editor de texto. Como mínimo, realice los cambios necesarios y guarde el archivo cuando haya terminado.

```
apiVersion: v1
data:
  .dockerconfigjson: ewoJCQkJImF1dGhzJUV2s1ZVZwWVFuWmp...
kind: Secret
metadata:
  creationTimestamp: "2020-11-12T02:41:08Z"
  managedFields:
  - apiVersion: v1
    ...
  name: harbor-registry-secret   #OPTIONAL: Change if desired
  namespace: default           #REQUIRED: Enter the Kuberentes namespace
  ownerReferences:
  - apiVersion: registryagent.vmware.com/v1alpha1
    ...
  resourceVersion: "675868"
  selfLink: /api/v1/namespaces/tkgs-cluster-ns/secrets/tkgs-cluster-ns-default-image-pull-
secret
  uid: 66606b41-7363-4b74-a3f2-4436f83f
type: kubernetes.io/dockerconfigjson
```

- OBLIGATORIO: Cambie el valor de `namespace` para que coincida con un espacio de nombres de Kubernetes adecuado del clúster, como **default**.

  Nota Para configurar el secreto de extracción de imágenes, especifique un espacio de nombres de Kubernetes. Si el clúster de Tanzu Kubernetes ya existe, cambie su contexto y ejecute `kubectl get namespaces` para enumerar los espacios de nombres de Kubernetes disponibles. Si es necesario, cree el espacio de nombres de destino antes de continuar. Si el clúster de Tanzu Kubernetes no existe, puede utilizar el espacio de nombres de `default`.

- OPCIONAL: cambie el valor de `name` por un nombre que tenga sentido, como **harbor-registry-secret** o **private-registry-secret**.

5 Cree un archivo kubeconfig que se pueda utilizar para acceder al clúster de Tanzu Kubernetes.

```
kubectl get secret -n <vsphere-namespace> <cluster-name>-kubeconfig -o
jsonpath='{.data.value}' | base64 -d > <path>/cluster-kubeconfig
```

Reemplace *<vsphere-namespace>* por el nombre del espacio de nombres de vSphere en el que se aprovisiona el clúster de Tanzu Kubernetes de destino. Reemplace *<cluster-name>* por el nombre del clúster de Tanzu Kubernetes.

```
kubectl get secret -n tkgs-cluster-ns tkgs-cluster-5-kubeconfig -o
jsonpath='{.data.value}' | base64 -d > tanzu/cluster-kubeconfig
```

6 Cree el secreto del servicio de registro en el clúster de Tanzu Kubernetes. Consulte el archivo del secreto de extracción de imágenes que guardó y actualizó en local.

```
kubectl --kubeconfig=<path>/cluster-kubeconfig apply -f <path>/image-pull-secret.yaml
```

Por ejemplo:

```
kubectl --kubeconfig=tanzu/cluster-kubeconfig apply -f tanzu/image-pull-secret.yaml
```

Debería ver que el secreto del servicio de registro se creó correctamente.

```
secret/harbor-registry-secret created
```

Configurar una carga de trabajo de Tanzu Kubernetes para extraer imágenes de un registro de contenedor privado

Para extraer imágenes de un registro de contenedor privado para una carga de trabajo del clúster de Tanzu Kubernetes, configure el YAML de carga de trabajo con los detalles del registro privado.

Este procedimiento se puede utilizar para extraer imágenes de un registro de contenedor privado o del registro de Harbor incrustado. En este ejemplo, creamos una especificación de pod que utilizará una imagen almacenada en el registro de Harbor integrado y utilizará el secreto de extracción de imágenes que se configuró anteriormente.

1 Cree un ejemplo de especificación de Pod con los detalles del registro privado.

```
apiVersion: v1
kind: Pod
metadata:
  name: <workload-name>
  namespace: <kubernetes-namespace>
spec:
  containers:
  - name: private-reg-container
    image: <Registry-IP-Address>/<vsphere-namespace>/<image-name>:<version>
  imagePullSecrets:
  - name: <registry-secret-name>
```

- Reemplace `<workload-name>` por el nombre de la carga de trabajo del pod.
- Reemplace `<kubernetes-namespace>` por el espacio de nombres de Kubernetes del clúster en el que se creará el pod. Debe ser el mismo espacio de nombres de Kubernetes en el que se almacena el secreto de extracción de imágenes del servicio de registro en el clúster de Tanzu Kubernetes (por ejemplo, el espacio de nombres predeterminado).
- Reemplace `<Registry-IP-Address>` por la dirección IP de la instancia del registro de Harbor integrado que se ejecuta en el clúster supervisor.
- Reemplace *<vsphere-namespace>* por el espacio de nombres de vSphere en el que se aprovisiona la instancia de Tanzu Kubernetes de destino.
- Reemplace `<image-name>` por el nombre de imagen que desee.
- Reemplace `<version>` por una versión adecuada de la imagen (por ejemplo, "más reciente").

- Reemplace `<registry-secret-name>` por el nombre del secreto de extracción de imágenes del servicio de registro que creó anteriormente.

2 Cree una carga de trabajo en el clúster de Tanzu Kubernetes basada en la especificación de pod que definió.

```
kubectl --kubeconfig=<path>/cluster-kubeconfig apply -f <pod.yaml>
```

El pod se debe crear a partir de la imagen extraída del registro.

Usar un registro de contenedor externo con clústeres de Tanzu Kubernetes

Puede utilizar un registro de contenedor externo con pods de clústeres de Tanzu Kubernetes. Se trata de una alternativa al uso de un registro de Harbor integrado.

Caso de uso de registro privado externo

Los registros de contenedores proporcionan una función crítica para las implementaciones de Kubernetes, y sirven como repositorio centralizado para almacenar y compartir imágenes de contenedor. El registro de contenedor público más utilizado es DockerHub. Existen muchas ofertas de registros de contenedores privados. VMware Harbor es un registro de contenedor privado, nativo en la nube y de código abierto. vSphere with Tanzu integra una instancia de Harbor que puede utilizar como registro de contenedor privado para pods de vSphere y para los pods que se ejecutan en clústeres de Tanzu Kubernetes. Para obtener más información, consulte Habilitar el registro de Harbor integrado en el clúster supervisor.

El registro de Harbor integrado que se incluye con vSphere with Tanzu requiere redes NSX-T. Si está utilizando redes de vSphere, no podrá utilizarlo. Además, es posible que ya esté ejecutando su propio registro de contenedor privado y que desee integrarlo con sus clústeres de Tanzu Kubernetes. En este caso, puede configurar el servicio Tanzu Kubernetes Grid para que confíe en registros privados con certificados autofirmados, lo que permite que los pods de Kubernetes que se ejecutan en clústeres de Tanzu Kubernetes utilicen el registro externo.

Requisitos del registro privado externo

Para usar un registro privado externo con clústeres de Tanzu Kubernetes, debe usar vSphere with Tanzu versión 7 U2 o posterior.

Solo puede utilizar su propio registro privado con pods de Kubernetes que se ejecuten en clústeres de Tanzu Kubernetes y máquinas virtuales del nodo de versión de Tanzu Kubernetes. No puede usar su propio registro privado con pods de vSphere que se ejecuten de forma nativa en hosts ESXi. El registro admitido para pods de vSphere es el registro de Harbor integrado en la plataforma de vSphere with Tanzu.

Una vez que configure el servicio Tanzu Kubernetes Grid para un registro privado, cualquier clúster nuevo que se aprovisione admitirá el registro privado. Para que los clústeres existentes admitan el registro privado, se requiere una actualización gradual para aplicar `TkgServiceConfiguration`. Consulte Actualizar clústeres de Tanzu Kubernetes. Además, la primera vez que cree una instancia personalizada de `TkgServiceConfiguration`, el sistema iniciará una actualización gradual.

Configuración del registro privado externo

Para utilizar su propio registro privado con clústeres de Tanzu Kubernetes, configure el servicio Tanzu Kubernetes Grid con uno o varios certificados autofirmados para que proporcione contenido de registro privado a través de HTTPS.

`TkgServiceConfiguration` se actualiza para admitir certificados autofirmados para el registro privado. Específicamente, se agrega una nueva sección de `trust` con el campo `additionalTrustedCAs`, lo que le permite definir un número cualquiera de certificados autofirmados en los que deberían confiar los clústeres de Tanzu Kubernetes. Esta funcionalidad permite definir fácilmente una lista de certificados y actualizar esos certificados en caso de que necesiten rotación.

Una vez que `TkgServiceConfiguration` se actualiza y se aplica, los certificados TLS se aplicarán a los clústeres nuevos la próxima vez que se cree un clúster. En otras palabras, la aplicación de una actualización a `TkgServiceConfiguration.trust.additionalTrustedCAs` no activa una actualización gradual automática de los clústeres de Tanzu Kubernetes.

```
apiVersion: run.tanzu.vmware.com/v1alpha1
kind: TkgServiceConfiguration
metadata:
  name: tkg-service-configuration
spec:
  defaultCNI: antrea
  trust:
    additionalTrustedCAs:
      - name: first-cert-name
        data: base64-encoded string of a PEM encoded public cert 1
      - name: second-cert-name
        data: base64-encoded string of a PEM encoded public cert 2
```

Para aplicar la actualización, ejecute el siguiente comando.

```
kubectl apply -f tkgserviceconfiguration.yaml
```

Debido a que la especificación de servicio Tanzu Kubernetes Grid se está actualizando con los certificados del registro privado, no es necesario agregar la clave pública al clúster de Tanzu Kubernetes kubeconfig como lo hace cuando utiliza el registro de Harbor integrado con clústeres de Tanzu Kubernetes.

Configurar una carga de trabajo de Tanzu Kubernetes para extraer imágenes de un registro de contenedor privado

Para extraer imágenes de un registro de contenedor privado para una carga de trabajo del clúster de Tanzu Kubernetes, configure el YAML de carga de trabajo con los detalles del registro privado.

Este procedimiento se puede utilizar para extraer imágenes de un registro de contenedor privado o del registro de Harbor incrustado. En este ejemplo, creamos una especificación de pod que utilizará una imagen almacenada en el registro de Harbor integrado y utilizará el secreto de extracción de imágenes que se configuró anteriormente.

1 Cree un ejemplo de especificación de Pod con los detalles del registro privado.

```
apiVersion: v1
kind: Pod
metadata:
  name: <workload-name>
  namespace: <kubernetes-namespace>
spec:
  containers:
  - name: private-reg-container
    image: <Registry-IP-Address>/<vsphere-namespace>/<image-name>:<version>
  imagePullSecrets:
  - name: <registry-secret-name>
```

- Reemplace <workload-name> por el nombre de la carga de trabajo del pod.
- Reemplace <kubernetes-namespace> por el espacio de nombres de Kubernetes del clúster en el que se creará el pod. Debe ser el mismo espacio de nombres de Kubernetes en el que se almacena el secreto de extracción de imágenes del servicio de registro en el clúster de Tanzu Kubernetes (por ejemplo, el espacio de nombres predeterminado).
- Reemplace <Registry-IP-Address> por la dirección IP de la instancia del registro de Harbor integrado que se ejecuta en el clúster supervisor.
- Reemplace *<vsphere-namespace>* por el espacio de nombres de vSphere en el que se aprovisiona la instancia de Tanzu Kubernetes de destino.
- Reemplace <image-name> por el nombre de imagen que desee.
- Reemplace <version> por una versión adecuada de la imagen (por ejemplo, "más reciente").
- Reemplace <registry-secret-name> por el nombre del secreto de extracción de imágenes del servicio de registro que creó anteriormente.

2 Cree una carga de trabajo en el clúster de Tanzu Kubernetes basada en la especificación de pod que definió.

```
kubectl --kubeconfig=<path>/cluster-kubeconfig apply -f <pod.yaml>
```

El pod se debe crear a partir de la imagen extraída del registro.

Campos de confianza para registros privados externos

Agregue una entrada de certificado (cadena con codificación Base64 de un certificado público con codificación PEM) a la sección `additionalTrustedCAs` de `TkgServiceConfiguration`. Los datos son certificados públicos almacenados en texto sin formato en TkgServiceConfiguration.

Tabla 15-1. Campos de confianza para registros privados

Campo	Descripción
`trust`	Marcador de sección. No acepta datos.
`additionalTrustedCAs`	Marcador de sección. Incluye una matriz de certificados con nombre y datos para cada uno.
`name`	El nombre del certificado de TLS.
`data`	La cadena codificada en base64 de un certificado público con codificación PEM.

Quitar certificados de registro privado externo

Elimine un certificado de la lista de certificados de la sección `additionalTrustedCAs` de `TkgServiceConfiguration` y aplique `TkgServiceConfiguration` al servicio Tanzu Kubernetes Grid.

Rotación de certificados de registro privado externo

Para rotar un certificado, el administrador de VI o el ingeniero de desarrollo y operaciones cambiaría el contenido del certificado en `TkgServiceConfiguration` o la especificación del clúster de Tanzu Kubernetes y aplicaría esa configuración para activar una actualización gradual de ese TKC.

Solucionar problemas de certificados de registro privado externo

Si configura el servicio Tanzu Kubernetes Grid con los certificados en los que confiar y agrega el certificado autofirmado al clúster kubeconfig, debería poder extraer correctamente una imagen de contenedor de un registro privado que use ese certificado autofirmado.

El siguiente comando puede ayudarle a determinar si la imagen del contenedor se extrajo correctamente para una carga de trabajo del pod:

```
kubectl describe pod PODNAME
```

Este comando muestra el estado detallado y los mensajes de error para un pod determinado. Un ejemplo de intento de extracción de una imagen antes de agregar certificados personalizados al clúster:

```

Events:
  Type     Reason                          Age               From               Message
  ----     ------                          ----              ----               -------
  Normal   Scheduled                       33s               default-scheduler  ...
```

```
  Normal   Image                        32s               image-controller   ...
  Normal   Image                        15s               image-controller   ...
  Normal   SuccessfulRealizeNSXResource  7s (x4 over 31s)  nsx-container-ncp  ...
  Normal   Pulling                      7s                kubelet            Waiting test-gc-
e2e-demo-ns/testimage-8862e32f68d66f727d1baf13f7eddef5a5e64bbd-v10612
  Warning  Failed                       4s                kubelet            failed to get
images: ... Error: ... x509: certificate signed by unknown authority
```

Y, al ejecutar el siguiente comando:

```
kubectl get pods
```

El error `ErrImagePull` también se puede ver en la vista de estado general del pod:

```

NAME                                          READY   STATUS         RESTARTS   AGE
testimage-nginx-deployment-89d4fcff8-2d9pz   0/1     Pending        0          17s
testimage-nginx-deployment-89d4fcff8-7kp9d   0/1     ErrImagePull   0          79s
testimage-nginx-deployment-89d4fcff8-7mpkj   0/1     Pending        0          21s
testimage-nginx-deployment-89d4fcff8-fszth   0/1     ErrImagePull   0          50s
testimage-nginx-deployment-89d4fcff8-sjnjw   0/1     ErrImagePull   0          48s
testimage-nginx-deployment-89d4fcff8-xr5kg   0/1     ErrImagePull   0          79s
```

Los errores “x509: certificado firmado por entidad desconocida” y “ErrImagePull” indican que el clúster no está configurado con el certificado correcto para conectarse al registro de contenedor privado. Falta el certificado o está mal configurado.

Si experimenta errores al conectarse a un registro privado después de configurar los certificados, puede comprobar si los certificados aplicados en la configuración se aplican al clúster. Puede comprobar si los certificados se aplicaron correctamente en su configuración mediante SSH.

Se pueden realizar dos pasos de investigación conectándose a un nodo de trabajador a través de SSH.

1 Compruebe la carpeta `/etc/ssl/certs/` en busca de archivos denominados `tkg-<cert_name>.pem`, donde `<cert_name>` es la propiedad "name" del certificado agregado en `TkgServiceConfiguration`. Si los certificados coinciden con lo que está presente en `TkgServiceConfiguration`, y sigue sin poder usarse un registro privado, complete el siguiente paso para profundizar en el diagnóstico.

2 Ejecute la siguiente prueba de conexión openssl con el servidor de destino mediante certificados autofirmados ejecutando el comando `openssl s_client -connect hostname:port_num`, donde hostname es el nombre de host o el nombre DNS del registro privado que utiliza certificados autofirmados, y port_num es el número de puerto en el que se ejecuta el servicio (por lo general, el puerto 443 para HTTPS). Puede comprobar exactamente qué error devuelve openssl cuando intenta conectarse al endpoint que utiliza certificados autofirmados y solucionar la situación desde allí; por ejemplo, agregando los certificados

correctos a `TkgServiceConfiguration`. Si el clúster de Tanzu Kubernetes está integrado con el certificado incorrecto, deberá actualizar la configuración de servicio Tanzu Kubernetes Grid con los certificados correctos, eliminar el clúster de Tanzu Kubernetes y, a continuación, volver a crearlo con la configuración que contiene los certificados correctos.

Trabajar con vSphere Lifecycle Manager

16

Como administrador de vSphere, puede habilitar vSphere with Tanzu en clústeres de vSphere que administre con una sola imagen de VMware vSphere Lifecycle Manager. A continuación, puede utilizar la instancia de clúster supervisor mientras vSphere Lifecycle Manager la administra.

vSphere Lifecycle Manager permite administrar los clústeres y los hosts ESXi en su entorno. Puede actualizar una instancia de clúster supervisor a la versión más reciente de vSphere with Tanzu. También puede actualizar la versión de ESXi de los hosts en el clúster supervisor.

vSphere Lifecycle Manager es un servicio que se ejecuta en vCenter Server. Cuando se implementa vCenter Server, la interfaz de usuario de vSphere Lifecycle Manager está habilitada en la instancia de vSphere Client basada en HML5.

Para obtener más información sobre vSphere Lifecycle Manager, consulte la documentación de *Administración del ciclo de vida de hosts y clústeres*.

Este capítulo incluye los siguientes temas:

- Requisitos
- Habilitar vSphere with Tanzu en un clúster administrado por vSphere Lifecycle Manager
- Actualizar una instancia de clúster supervisor
- Agregar hosts a un clúster supervisor
- Quitar hosts de clúster supervisor
- Deshabilitar una instancia de Supervisor Cluster

Requisitos

Para configurar vSphere with Tanzu en un clúster de vSphere que administre vSphere Lifecycle Manager, el entorno debe cumplir determinados requisitos.

Requisitos del sistema

Para habilitar vSphere with Tanzu, compruebe que los componentes del clúster de vSphere cumplan los siguientes requisitos:

- Compruebe que vCenter Server y ESXi sean de la versión 7.0 Update 2 si usa NSX-T Data Center.

- Compruebe que vCenter Server y ESXi sean de la versión 7.0 Update 1 como mínimo si usa Redes de vSphere.
- Compruebe que todos los hosts ESXi que desee utilizar como parte de una instancia de clúster supervisor tengan asignada una licencia de VMware vSphere 7 Enterprise Plus con el complemento para Kubernetes.
- Compruebe que HA y DRS estén habilitados en el clúster de vSphere.
- Compruebe que vSphere Distributed Switch 7.0 Update 2 esté configurado.
- Compruebe que Redes de vSphere o NSX-T Data Center 3.1 o una versión posterior esté configurado en el clúster. No puede utilizar una imagen de vSphere Lifecycle Manager para administrar un clúster que esté configurado con versiones anteriores de NSX-T Data Center.

Habilitar vSphere with Tanzu en un clúster administrado por vSphere Lifecycle Manager

Para ejecutar cargas de trabajo de Kubernetes, puede habilitar vSphere with Tanzu en un clúster que administre con una sola imagen de vSphere Lifecycle Manager. Una vez habilitado, puede administrar clúster supervisor mediante vSphere Lifecycle Manager.

Cuando se habilita el clúster con vSphere with Tanzu que utiliza NSX-T Data Center, vSphere Lifecycle Manager instala el paquete de instalación de vSphere de Spherelet (VIB) en cada host ESXi del clúster. Al habilitar el clúster, se asigna la versión de Kubernetes que se incluye con vCenter. Una vez finalizada la instalación, el servicio WCP realiza las tareas posteriores a la instalación, como iniciar y configurar Spherelet.

Para conocer los pasos para habilitar el clúster, consulte Habilitar la administración de cargas de trabajo con redes de vSphere.

Actualizar una instancia de clúster supervisor

Puede actualizar a la versión más reciente de vSphere with Tanzu, incluida la infraestructura de vSphere compatible con clústeres de vSphere with Tanzu, las versiones de Kubernetes y las herramientas de CLI de Kubernetes para vSphere en los clústeres que usan una imagen de vSphere Lifecycle Manager única.

Actualice la versión de ESXi de los hosts en el clúster supervisor. Durante la actualización, se actualiza el VIB de Spherelet en cada host ESXi.

vSphere Lifecycle Manager utiliza DRS y pone los hosts en modo de mantenimiento antes de la corrección. Para que la corrección sea exitosa, DRS primero intenta migrar a otro host la máquina virtual que ejecuta vCenter Server (por ejemplo, las máquinas virtuales que tienen afinidad con el host o que se ejecutan en el almacenamiento local del host) y las cargas de trabajo, incluidos los pods de vSphere, a otros hosts.

Nota Puede usar vSphere Lifecycle Manager para actualizar una instancia de clúster supervisor solo en clústeres que usan una sola imagen de vSphere Lifecycle Manager.

Procedimiento

1 En el menú vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione la pestaña **Actualizaciones**.

3 Seleccione la **Versión disponible** a la que desea actualizar.

   Por ejemplo, seleccione la versión `v1.17.4-vsc0.0.2-16293900`.

4 Seleccione la instancia de clúster supervisor a la que se aplicará la actualización.

5 Para iniciar la actualización, haga clic en **Aplicar actualizaciones**.

6 Utilice el panel **Tareas recientes** para supervisar el estado de la actualización.

Agregar hosts a un clúster supervisor

Como administrador de vSphere, es posible que tenga que escalar horizontalmente la instancia de clúster supervisor para ejecutar más cargas de trabajo. Para agregar capacidad a un clúster, puede agregar hosts ESXi al clúster que utiliza una sola imagen de vSphere Lifecycle Manager.

Cuando agregue un host al clúster supervisor configurado con NSX-T Data Center, vSphere Lifecycle Manager instala el Spherelet VIB y la imagen en el host. Una vez instalado, vSphere with Tanzu configura el proceso de Spherelet en el host que se acaba de agregar, el cual permite ejecutar contenedores de forma nativa en ESXi.

Requisitos previos

- Obtenga el nombre de usuario y la contraseña de la cuenta de usuario raíz para el host.
- Compruebe que los hosts que se encuentran detrás de un firewall puedan comunicarse con vCenter Server.

Procedimiento

1 En el menú vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Haga clic con el botón derecho en el centro de datos, el clúster o la carpeta y seleccione **Agregar host**.

3 Introduzca la dirección IP o el nombre del host y haga clic en **Siguiente**.

4 Introduzca las credenciales de administrador y haga clic en **Siguiente**.

5 Revise el resumen del host y haga clic en **Siguiente**.

6 Asigne una licencia al host y haga clic en **Finalizar**.

7 En el asistente **Agregar host**, haga clic en **Siguiente**.

8 Revise el resumen y haga clic en **Finalizar**.

   Nota Si un host forma parte del mismo centro de datos, puede moverlo a clúster supervisor. Para mover el host, póngalo en modo de mantenimiento y arrástrelo al clúster.

Quitar hosts de clúster supervisor

Como administrador de vSphere, es posible que tenga que reducir horizontalmente la instancia de clúster supervisor para ahorrar costes. Para reducir la capacidad de una clúster supervisor, puede quitar los hosts ESXi de un clúster que utilice una sola imagen de vSphere Lifecycle Manager.

Cuando se elimina un host de clúster supervisor configurado con NSX-T Data Center, vSphere with Tanzu borra la configuración de Spherelet y detiene el proceso de Spherelet en el host ESXi. A continuación, vSphere Lifecycle Manager desinstala la imagen y el VIB de Spherelet del host y vSphere with Tanzu elimina los metadatos del host del plano de control del clúster.

Requisitos previos

Antes de quitar un host de un clúster, debe apagar todas las máquinas virtuales que se están ejecutando en el host o bien migrar las máquinas virtuales a un nuevo host.

Procedimiento

1 En vSphere Client, desplácese hasta el clúster del que desea quitar el host.

2 Haga clic con el botón derecho en el host y seleccione **Entrar en modo de mantenimiento** en el menú desplegable.

3 En el cuadro de diálogo de confirmación que aparece, haga clic en **Sí**.

   En el cuadro de diálogo de confirmación también se pregunta si desea mover las máquinas virtuales que estén apagadas a otros hosts. Seleccione esta opción si desea que esas máquinas virtuales permanezcan registradas en un host del clúster.

   El icono del host cambia y se agrega el término "modo de mantenimiento" al nombre, entre paréntesis.

4 Seleccione el icono del host en el inventario y arrástrelo a la nueva ubicación.

   El host puede moverse a otro clúster o centro de datos.

   vCenter Server mueve el host a la nueva ubicación.

5 Haga clic con el botón derecho en el host y seleccione **Salir del modo de mantenimiento** en el menú desplegable.

6 (opcional) Reinicie las máquinas virtuales, en caso necesario.

Deshabilitar una instancia de Supervisor Cluster

vSphere with Tanzu se puede deshabilitar de un clúster de vSphere que utiliza una sola imagen de vSphere Lifecycle Manager para que esté disponible para las cargas de trabajo tradicionales.

Cuando se deshabilita un vSphere with Tanzu en un clúster, vSphere Lifecycle Manager desinstala el VIB y la imagen de Spherelet de cada host ESXi, y el servicio de `WCP` se detiene y elimina todas las cargas de trabajo del clúster.

Procedimiento

1 En el menú vSphere Client, seleccione **Administración de cargas de trabajo**.

2 Seleccione la pestaña **Clústeres**.

3 Seleccione el clúster en el que desea deshabilitar vSphere with Tanzu.

4 Haga clic en **Deshabilitar**.

   Aparecerá el cuadro de diálogo **Deshabilitar clúster** con un mensaje donde se indica que todas las cargas de trabajo de Kubernetes y la configuración de NSX-T Data Center se deshabilitarán en el clúster.

5 Haga clic en **Deshabilitar**.

Actualizar el entorno de vSphere with Tanzu

17

Puede actualizar a la versión más reciente de vSphere with Tanzu, incluidas la infraestructura de vSphere que respalda los clústeres de vSphere with Tanzu, las versiones de Kubernetes y la instancia de Herramientas de la CLI de Kubernetes para vSphere.

Este capítulo incluye los siguientes temas:

- Acerca de las actualizaciones de vSphere with Tanzu
- Actualización de la topología de red
- Actualizar clúster supervisor mediante una actualización de los espacios de nombres de vSphere
- Actualización automática de clúster supervisor
- Actualizar complemento de vSphere para kubectl
- Comprobar la compatibilidad del clúster de Tanzu Kubernetes para actualizar
- Actualizar clústeres de Tanzu Kubernetes

Acerca de las actualizaciones de vSphere with Tanzu

vSphere with Tanzu admite actualizaciones graduales para los clústeres supervisor y los clústeres de servicio Tanzu Kubernetes Grid, así como para la infraestructura que respalda estos clústeres.

Cómo se actualizan los clústeres supervisory los clústeres de servicio Tanzu Kubernetes Grid

vSphere with Tanzu utiliza un modelo de actualización gradual para los clústeres supervisor y los clústeres de servicio Tanzu Kubernetes Grid. El modelo de actualización gradual garantiza un tiempo de inactividad mínimo para las cargas de trabajo del clúster durante el proceso de actualización. Las actualizaciones graduales incluyen la actualización de las versiones de software de Kubernetes, así como de la infraestructura y los servicios que respaldan los clústeres de Kubernetes, como los recursos y las configuraciones de máquinas virtuales, los servicios y los espacios de nombres de vSphere, y los recursos personalizados.

Para que la actualización se realice correctamente, la configuración debe cumplir con varios requisitos de compatibilidad, de modo que el sistema aplique condiciones de reverificación a fin de garantizar que los clústeres estén listos para las actualizaciones y que dicho sistema sea compatible con la reversión si el clúster no se actualiza correctamente.

Nota Una actualización de vSphere with Tanzu implica más que la actualización de la versión de software de Kubernetes. Cuando hablamos de "actualización" nos referimos a este proceso y no a la forma limitada de actualización que incrementa la versión de software.

Dependencia entre las actualizaciones de clúster supervisor y las actualizaciones de clústeres de servicio Tanzu Kubernetes Grid

Debe actualizar el clúster supervisor y los clústeres de servicio Tanzu Kubernetes Grid por separado. Sin embargo, tenga en cuenta que existen dependencias entre los dos.

La actualización de un clúster supervisor probablemente active una actualización gradual de los clústeres de servicio Tanzu Kubernetes Grid implementados allí. Consulte Actualizar clúster supervisor mediante una actualización de los espacios de nombres de vSphere.

Es posible que deba actualizar uno o varios clústeres de servicio Tanzu Kubernetes Grid antes de actualizar un clúster supervisor si el clúster de servicio Tanzu Kubernetes Grid no es compatible con la versión de clúster supervisor de destino. Consulte Comprobar la compatibilidad del clúster de Tanzu Kubernetes para actualizar.

Acerca de las actualizaciones de clúster supervisor

Cuando se inicia una actualización de una instancia de clúster supervisor, el sistema crea un nuevo nodo de plano de control y lo une al plano de control existente. El inventario de vSphere muestra cuatro nodos del plano de control durante esta fase de la actualización, ya que el sistema agrega un nuevo nodo actualizado y, a continuación, elimina el nodo antiguo obsoleto. Los objetos se migran a partir de uno de los nodos del plano de control antiguos hacia el nuevo, mientras que el nodo antiguo del plano de control se elimina. Este proceso se repite de a un nodo por vez hasta que se actualizan todos los nodos del plano de control. Una vez actualizado el plano de control, los nodos de trabajo pasan por un tipo de actualización gradual similar. Los nodos de trabajo son los hosts ESXi y cada proceso de Spherelet en cada host ESXi se actualiza de uno en uno.

Puede elegir entre las siguientes actualizaciones:

- Actualice los espacios de nombres de vSphere.
- Actualice todo, incluidas las versiones de VMware y las versiones de Kubernetes.

Puede usar el flujo de trabajo de actualización de espacios de nombres de vSphere para actualizar la versión de Kubernetes que se está ejecutando en el clúster supervisor (por ejemplo, de Kubernetes 1.16.7 a Kubernetes 1.17.4) y la infraestructura que respalda el clúster supervisor y los clústeres de servicio Tanzu Kubernetes Grid. Este tipo de actualización es más frecuente y se utiliza para mantener el ritmo de la cadencia de versiones de Kubernetes. A continuación se muestra la secuencia de actualización de los espacios de nombres de vSphere.

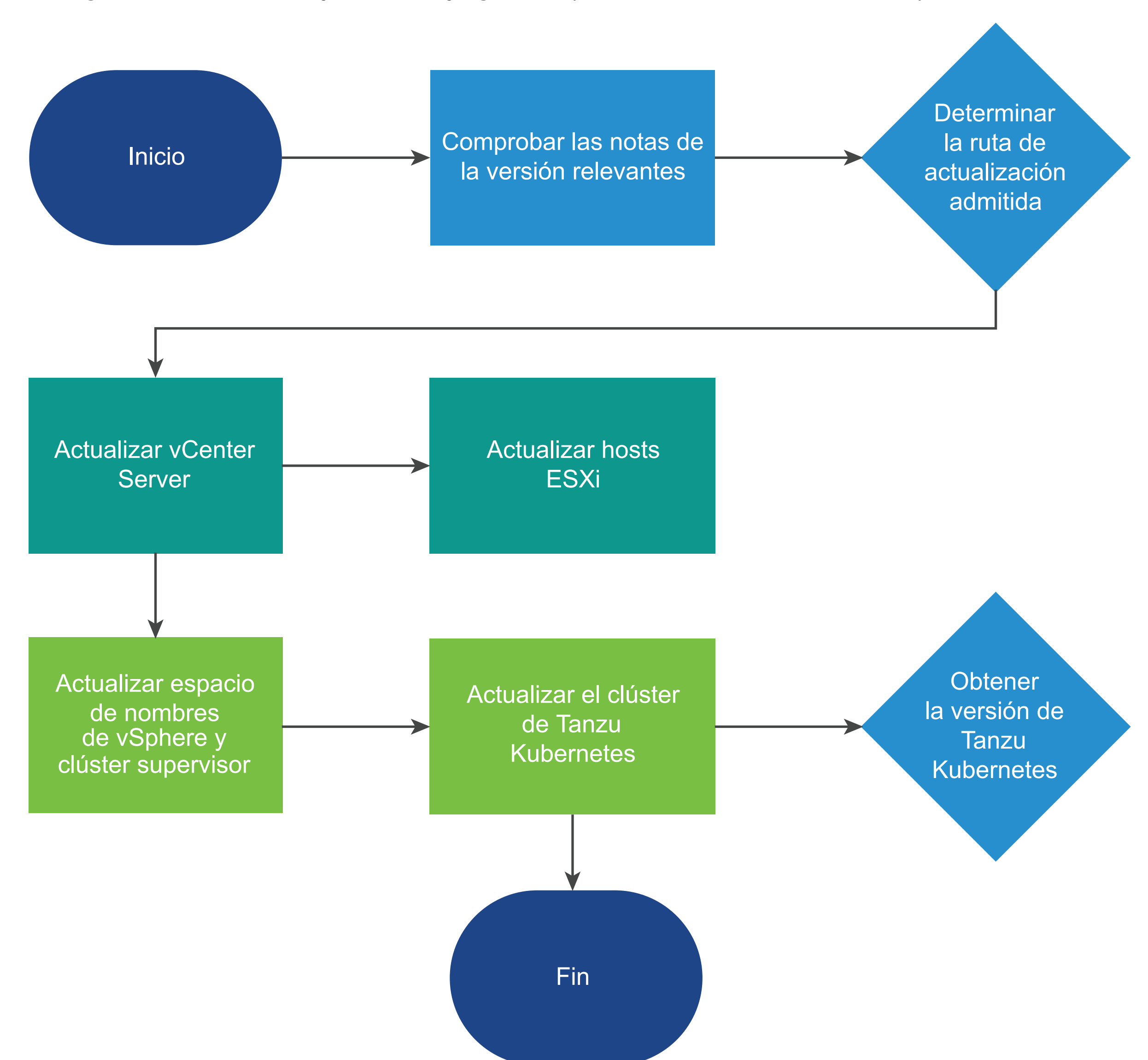
1 Actualice vCenter Server.
2 Realice una actualización de los espacios de nombres de vSphere (incluida la actualización de Kubernetes).

Para realizar una actualización de espacios de nombres de vSphere, consulte Actualizar clúster supervisor mediante una actualización de los espacios de nombres de vSphere.

Utilice el flujo de trabajo de actualización total para actualizar todos los componentes de vSphere with Tanzu. Este tipo de actualización es necesaria cuando se actualizan versiones principales; por ejemplo, de NSX-T 3.X a 4 y de vSphere 7.X a 8. Este flujo de trabajo de actualización no es frecuente en función de cuándo hay nuevas versiones de productos de VMware. Esta es la secuencia de actualización total:

1 Compruebe la matriz de interoperabilidad de VMware https://interopmatrix.vmware.com/Interoperability para determinar la compatibilidad de vCenter Server y NSX-T Data Center. La funcionalidad de vSphere with Tanzu se proporciona mediante el software de plano de control de carga de trabajo (WCP) que se envía con vCenter Server.
2 Actualice NSX-T Data Center, si es compatible.
3 Actualice vCenter Server.
4 Actualice vSphere Distributed Switch.
5 Actualice los hosts ESXi.
6 Compruebe la compatibilidad de los clústeres de servicio Tanzu Kubernetes Grid aprovisionados con la versión del clúster supervisor de destino.
7 Actualice los espacios de nombres de vSphere (incluida la versión de Kubernetes de clúster supervisor).
8 Actualice los clústeres de servicio Tanzu Kubernetes Grid.

El diagrama muestra el flujo de trabajo general para las actualizaciones de vSphere with Tanzu.



Acerca de las actualizaciones de clústeres de servicio Tanzu Kubernetes Grid

Cuando se actualiza una instancia de clúster supervisor, también se actualizan los componentes de infraestructura que respaldan los clústeres de servicio Tanzu Kubernetes Grid implementados en esa instancia de clúster supervisor, como el servicio Tanzu Kubernetes Grid. Cada actualización de infraestructura puede incluir actualizaciones de los servicios que respaldan servicio Tanzu Kubernetes Grid (CNI, CSI y CPI) y opciones de configuración actualizadas para los nodos de trabajo y el plano de control que se pueden aplicar a los clústeres de servicio Tanzu Kubernetes Grid existentes. Para garantizar que la configuración cumpla con los requisitos de compatibilidad, vSphere with Tanzu realiza comprobaciones previas durante la actualización gradual y aplica la conformidad.

Para realizar una actualización gradual de un clúster de servicio Tanzu Kubernetes Grid, debe actualizar el manifiesto del clúster. Consulte Actualizar clústeres de Tanzu Kubernetes. Sin embargo, tenga en cuenta que, cuando se actualizan los espacios de nombres de vSphere, el sistema propaga de inmediato las configuraciones actualizadas a todos los clústeres de servicio Tanzu Kubernetes Grid. Estas actualizaciones pueden activar automáticamente una actualización gradual de los nodos de trabajo y de los nodos del plano de control de servicio Tanzu Kubernetes Grid.

El proceso de actualización gradual para reemplazar los nodos del clúster es similar a la actualización gradual de pods de una implementación de Kubernetes. Dos controladoras distintas se encargan de realizar una actualización gradual de los clústeres de servicio Tanzu Kubernetes Grid: la controladora de complementos y la controladora de TanzuKubernetesCluster. Dentro de esas dos controladoras hay tres etapas clave de una actualización gradual: la actualización de los complementos, la actualización del plano de control y la actualización de los nodos de trabajo. Estas etapas se producen en orden, con comprobaciones previas que impiden que un paso comience hasta que el paso anterior haya avanzado lo suficiente. Es posible que estos pasos se omitan si se determina que son innecesarios. Por ejemplo, una actualización podría solo afectar a los nodos de trabajo y, por tanto, no necesitaría actualizaciones de los planos de control ni de los complementos.

Durante el proceso de actualización, el sistema agrega un nuevo nodo de clúster y espera a que el nodo se conecte con la versión de Kubernetes de destino. A continuación, el sistema marca el nodo antiguo para su eliminación, pasa al siguiente nodo y repite el proceso. El nodo antiguo no se eliminará hasta que se eliminen todos los pods. Por ejemplo, si un pod se define con PodDisruptionBudgets que impide que un nodo se vacíe completamente, el nodo se acordona, pero no se elimina hasta que dichos pods se puedan expulsar. El sistema actualiza primero todos los nodos del plano de control y, a continuación, los nodos de trabajo. Durante una actualización, el estado del clúster de servicio Tanzu Kubernetes Grid cambia a "Actualizando". Una vez finalizado el proceso de actualización gradual, el estado del clúster de servicio Tanzu Kubernetes Grid cambia a "En ejecución".

Los pods en ejecución en un clúster de servicio Tanzu Kubernetes Grid que no están regidos por una controladora de replicación se eliminarán durante la actualización de la versión de Kubernetes como parte de la purga de nodos de trabajo al actualizar el clúster de servicio Tanzu Kubernetes Grid. Esto sucede si la actualización del clúster se activa de forma manual o de forma automática por una actualización de espacios de nombres de vSphere. Los pods que no están regidos por una controladora de replicación incluyen aquellos pods que no se crean como parte de una especificación de ReplicaSet o de implementación. Para obtener más información, consulte el tema Ciclo de vida del pod: duración del pod en la documentación de Kubernetes.

Actualización de la topología de red

Cuando instale vSphere with Tanzu versión 7.0 Update 1c o actualice el clúster supervisor de la versión 7.0 Update 1 a la versión 7.0 Update 1c, debe actualizar el complemento de contenedor de NSX (NSX Container Plug-in, NCP). A su vez, migra la topología de redes del clúster supervisor, los espacios de nombres y los clústeres de Tanzu Kubernetes. Después de la actualización, la

topología de red se actualiza desde una topología de puerta de enlace de nivel 1 única a una topología que tiene una puerta de enlace de nivel 1 para cada espacio de nombres dentro del clúster supervisor.

Durante la actualización, NCP configura los recursos de NSX-T Data Center para que sean compatibles con la nueva topología. NCP proporciona una infraestructura de red compartida para los espacios de nombres que tengan menos servicios de equilibrio de carga de capa 4 y capa 7. De este modo se reducen los recursos en NSX y hay más disponibles para los clústeres de Tanzu Kubernetes.

Los espacios de nombres del sistema son espacios de nombres que utilizan los componentes principales que son esenciales para el funcionamiento de los clústeres de clúster supervisor y Tanzu Kubernetes. Los recursos de red compartidos que incluyen la puerta de enlace de nivel 1, el equilibrador de carga y la IP de SNAT se agrupan en un espacio de nombres del sistema.

NCP crea de forma predeterminada una puerta de enlace de nivel 1 compartida para los espacios de nombres del sistema y una puerta de enlace de nivel 1 y un equilibrador de carga para cada espacio de nombres. La puerta de enlace de nivel 1 está conectada a la puerta de enlace de nivel 0 y a un segmento predeterminado.

El equilibrador de carga de NSX-T proporciona servicios de equilibrio de carga en forma de servidores virtuales.

Tras la migración, la topología de red tiene las siguientes características:

- Cada espacio de nombres de vSphere tiene una red independiente y un conjunto de recursos de red compartidos por las aplicaciones que están dentro del espacio de nombres, como la puerta de enlace de nivel 1, el servicio de equilibrador de carga y la dirección IP de SNAT.
- Las cargas de trabajo que se ejecutan en pods de vSphere, máquinas virtuales normales o clústeres de Tanzu Kubernetes, los cuales están en el mismo espacio de nombres, comparten una misma IP de SNAT para la conectividad de norte a sur.
- Las cargas de trabajo que se ejecutan en clústeres de pods de vSphere o Tanzu Kubernetes tendrán la misma regla de aislamiento que implementa el firewall predeterminado.
- No se requiere una IP de SNAT independiente para cada espacio de nombres de Kubernetes. La conectividad de este a oeste entre espacios de nombres no será SNAT.

La cantidad máxima de espacios de nombres que se pueden ejecutar depende del tamaño del nodo de Edge (mediano, grande o extragrande) y de la cantidad de nodos de Edge que haya en el clúster de NSX Edge. La cantidad de espacios de nombres que se pueden ejecutar es inferior a 20 veces la cantidad de nodos de Edge. Por ejemplo, si el clúster de NSX Edge tiene 10 nodos de Edge de tamaño grande, el número máximo de espacios de nombres de supervisor que se pueden crear es 199.

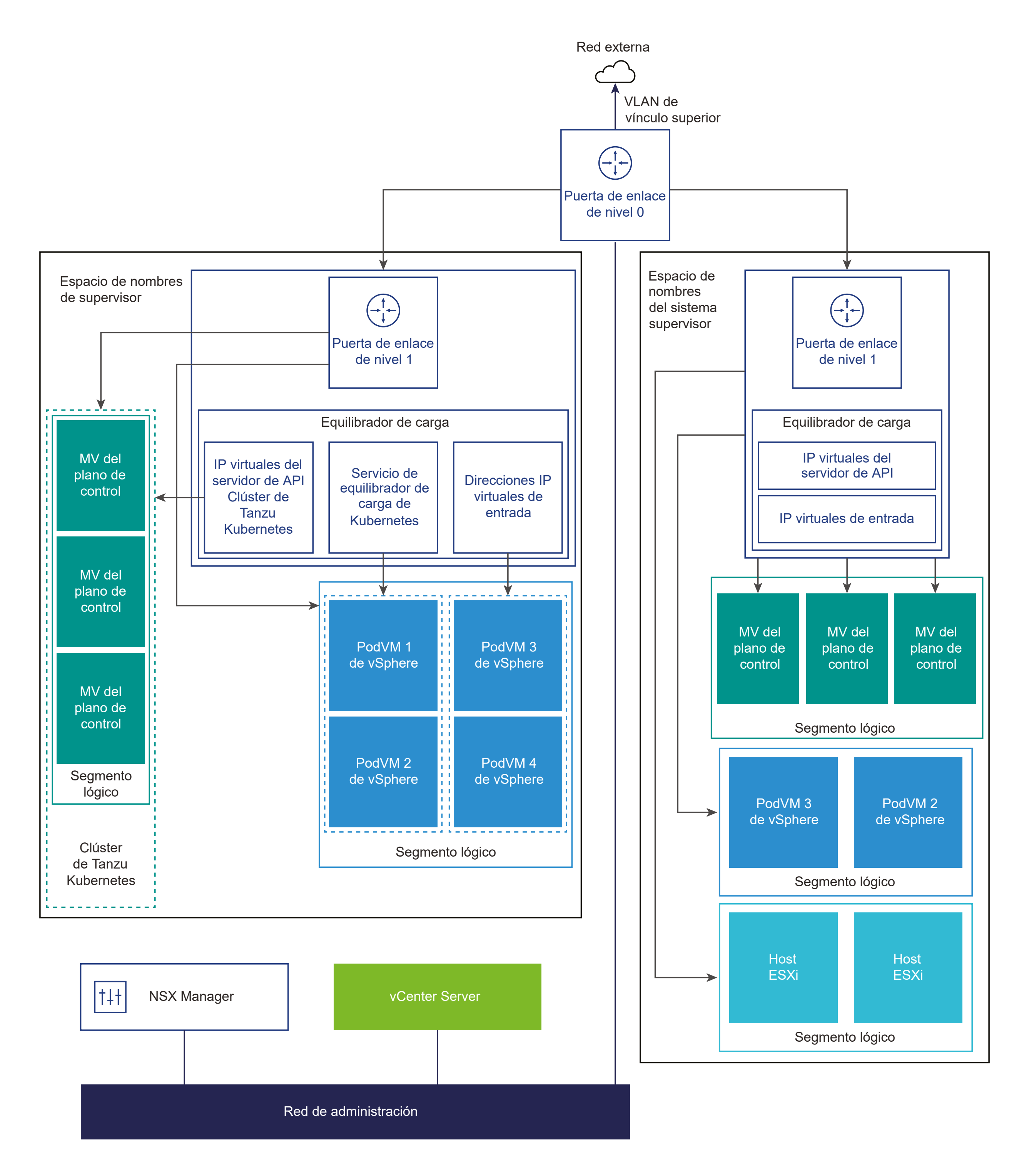
Para obtener más información sobre el tamaño del nodo de Edge, consulte la *Guía de instalación de NSX-T Data Center*.

Redes de clústeres supervisores

Los clústeres de supervisor tienen segmentos separados dentro de la puerta de enlace de nivel 1 compartida. Para cada clúster de Tanzu Kubernetes, los segmentos se definen en la puerta de enlace de nivel 1 del espacio de nombres.

Las cargas de trabajo, incluidos los pods de vSphere y los clústeres de Tanzu Kubernetes, los cuales están dentro del mismo espacio de nombres, compartirán una IP de SNAT para la conectividad de norte a sur. La conectividad de este a oeste entre espacios de nombres no será SNAT.

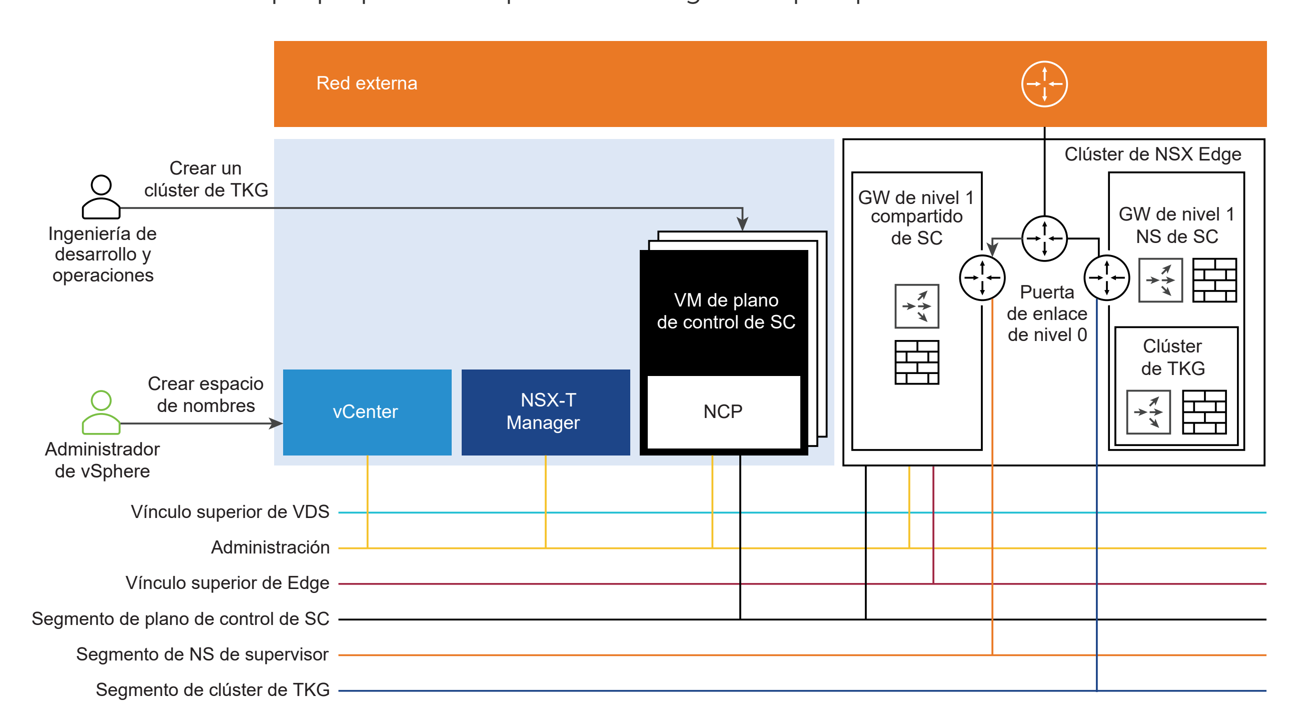
Figura 17-1. Redes de clústeres supervisores



Redes de clústeres de Tanzu Kubernetes

Después de la actualización del clúster supervisor, cuando los ingenieros de desarrollo y operaciones aprovisionan el primer clúster de Tanzu Kubernetes en un espacio de nombres de supervisor, el clúster compartirá la misma puerta de enlace de nivel 1 y el mismo equilibrador de carga que el espacio de nombres. Para cada clúster de Tanzu Kubernetes que se aprovisiona en ese espacio de nombres, se crea un segmento para ese clúster y se conecta a la puerta de enlace de nivel 1 compartida de su espacio de nombres de supervisor.

Cuando servicio Tanzu Kubernetes Grid aprovisiona un clúster de Tanzu Kubernetes, se crea un único servidor virtual que proporciona el equilibrio de carga de capa 4 para la API de Kubernetes. Este servidor virtual está alojado en el equilibrador de carga compartido con el espacio de nombres y es responsable de enrutar el tráfico de kubectl al plano de control. Asimismo, para cada equilibrador de carga del servicio de Kubernetes que obtiene recursos en el clúster, se crea un servidor virtual que proporciona equilibrio de carga de capa 4 para ese servicio.



Actualizar la topología de red de NSX-T

Para actualizar la topología de red, debe actualizar NSX-T Data Center, vCenter Server y todos los componentes de vSphere with Tanzu.

Puede actualizar la versión de NSX-T Data Center. Cuando se realiza la actualización, los componentes de NSX-T Data Center, que incluyen el plano de datos, el plano de control y el plano de administración, se actualizan con un mínimo tiempo de inactividad del sistema.

Para obtener información detallada sobre la actualización de los componentes de NSX-T Data Center, consulte la Guía de actualización de NSX-T Data Center.

Nota Consulte las Notas de la versión de vSphere with Tanzu para ver las versiones compatibles.

Requisitos previos

- Compruebe que el entorno cumpla con los requisitos del sistema. Para obtener información sobre los requisitos, consulte Requisitos del sistema para configurar vSphere with Tanzu con NSX-T Data Center.
- Para conocer los límites de configuración específicos de vSphere with Tanzu, consulte los límites de configuración de vSphere en la herramienta Valores máximos de configuración de VMware.

Procedimiento

1 Actualice NSX-T Data Center desde NSX-T Data Center 3.0.x a NSX-T Data Center 3.1.

2 Actualice vCenter Server.

3 Actualice los hosts ESXi.

4 Actualice el espacio de nombres del supervisor.

   Para realizar una actualización, consulte Actualizar clúster supervisor mediante una actualización de los espacios de nombres de vSphere.

Actualizar vSphere Distributed Switch

Es posible actualizar vSphere Distributed Switch versión 7.0 a una versión posterior. La actualización de un conmutador distribuido hace que los hosts y las máquinas virtuales asociados al conmutador experimenten un tiempo de inactividad breve.

Requisitos previos

- Actualizar vCenter Server a la versión 7.0.
- Actualice todos los hosts conectados al conmutador distribuido a ESXi 7.0.

Procedimiento

1 En el menú de inicio de vSphere Client, seleccione **Hosts y clústeres**.

2 Seleccione **Redes** y desplácese hasta el conmutador distribuido.

   Por ejemplo, **DSwitch**.

   La interfaz de usuario de vSphere Client enumera las versiones disponibles a las que se puede actualizar.

3 En el menú **Acciones**, seleccione **Actualizar > Actualizar Distributed Switch**.

4 Seleccione la versión de vSphere Distributed Switch a la que desee actualizar el conmutador y haga clic en Siguiente.

5 Revise la compatibilidad de host y haga clic en **Siguiente**.

6 Complete la configuración de actualización y haga clic en **Finalizar**.

Actualizar clúster supervisor mediante una actualización de los espacios de nombres de vSphere

Para actualizar uno o varios clústeres supervisor, incluida la versión de Kubernetes que el clúster supervisor está ejecutando y la infraestructura que respalda los clústeres de Tanzu Kubernetes, incluido servicio Tanzu Kubernetes Grid, debe realizar una actualización de los espacios de nombres de vSphere.

Existe una entidad de versión para vSphere with Tanzu. La entidad de versión es una cadena de versión semántica con el formato `v1.19.1+vmware.2-vsc0.0.8-17610687`, donde el prefijo es la versión de Kubernetes (`v1.19.1`) y el sufijo es la versión de los espacios de nombres de vSphere (`vsc0.0.8-17610687`).

En la tabla, se muestran las versiones de clúster supervisor disponibles:

Versión	Descripción
`v1.19.1+vmware.2-vsc0.0.8-17610687`	Versión de clúster supervisor más reciente; admite vSphere 7.0 Update 2.
`v1.18.2-vsc0.0.5-16762486`	Admite vSphere 7.0 Update 1.
`v1.17.4-vsc0.0.5-16762486`	Versión mínima de clúster supervisor que incluye una instancia de servicio Tanzu Kubernetes Grid que admite Antrea CNI.
`v1.16.7-vsc0.0.5-16762486`	Si va a ejecutar esta versión, debe actualizarla a 1.17 como mínimo.

Requisitos previos

Lea las notas de la versión antes de realizar una actualización de los espacios de nombres de vSphere.

Para instalar los archivos binarios necesarios, actualice el dispositivo de vCenter Server y los hosts ESXi a la versión compatible. Consulte Actualizar vCenter Server Appliance en la documentación de vCenter Server.

Nota Cuando se realiza una actualización de los espacios de nombres de vSphere, todos los clústeres de Tanzu Kubernetes aprovisionados deben estar en el estado en ejecución. Si un clúster de Tanzu Kubernetes se encuentra en un estado de creación o eliminación, espere a que finalice el proceso antes de actualizar una instancia de clúster supervisor; de lo contrario, es posible que no se complete correctamente.

Nota La actualización de un clúster supervisor probablemente active una actualización gradual de los clústeres de Tanzu Kubernetes implementados allí. Consulte Actualizar clústeres de Tanzu Kubernetes.

Procedimiento

1 Inicie sesión en vCenter Server como administrador de vSphere.

2 Seleccione **Menú > Administración de cargas de trabajo**.

3 Seleccione la pestaña **Espacios de nombres > Actualizaciones**.

4 Seleccione la **Versión disponible** a la que desea actualizar.

   Por ejemplo, seleccione la versión `v1.18.2-vsc0.0.5-16762486`.

   Nota Debe actualizar de forma incremental. No omita actualizaciones; por ejemplo, no debe actualizar de la versión 1.16 a la 1.18. El orden debe ser 1.16, 1.17 y 1.18.

5 Seleccione uno o varios clústeres supervisor donde aplicará la actualización.

6 Para iniciar la actualización, haga clic en **Aplicar actualizaciones**.

7 Utilice el panel **Tareas recientes** para supervisar el estado de la actualización.

Actualización automática de clúster supervisor

Puede actualizar automáticamente el clúster supervisor cuando actualice el dispositivo de vCenter Server.

Los componentes de vSphere with Tanzu incluyen componentes en vCenter Server, componentes de Kubernetes y componentes de ESXi. Cuando actualiza vCenter Server, solo se actualizan los componentes de vSphere with Tanzu en vCenter Server. Debe actualizar manualmente los componentes de Kubernetes y los de ESXi.

Con la función de actualización automática, cuando actualice vCenter Server, puede actualizar automáticamente el clúster supervisor. Para obtener una lista de las versiones de vCenter Server, consulte el siguiente artículo de la base de conocimientos: https://kb.vmware.com/s/article/2143838.

Cuando actualice el vCenter Server, se ejecutan comprobaciones previas para comprobar la compatibilidad entre el clúster supervisor y el vCenter Server. Las advertencias se muestran en los siguientes escenarios:

- La versión de Kubernetes del vCenter Server de destino puede provocar que clúster supervisor quede retrasado una versión. En este escenario, cuando se continúa con la actualización de vCenter Server, el clúster se actualiza automáticamente.

  Por ejemplo, la versión de clúster supervisor es 1.16 y la versión de vCenter Server de destino es 1.17, 1.18 o 1.19.

- La versión de Kubernetes de vCenter Server de destino puede provocar que clúster supervisor quede retrasado más de una versión. En este escenario, el vCenter Server no se actualiza.

  Por ejemplo, la versión de clúster supervisor es 1.15 y la versión de vCenter Server destino es 1.17, 1.18 o 1.19.

- La licencia de clúster supervisor ha caducado. En este escenario, si continúa con la actualización de vCenter Server, el clúster supervisor con la licencia caducada se vuelve inutilizable e irrecuperable.

Actualizar complemento de vSphere para kubectl

Una vez que haya realizado una actualización de espacio de nombres de vSphere y actualizado el clúster supervisor, actualice el complemento de vSphere para kubectl.

La versión más reciente de complemento de vSphere para kubectl descarga e instala el certificado de CA raíz del clúster de Tanzu Kubernetes en el secreto de Kubernetes denominado `TANZU-KUBERNETES-CLUSTER-NAME-ca`. El complemento utiliza este certificado para rellenar la información de CA en el almacén de datos de la entidad de certificación del clúster correspondiente.

Para descargar e instalar complemento de vSphere para kubectl, consulte Descargar e instalar Herramientas de la CLI de Kubernetes para vSphere. Para obtener más información sobre el secreto `TANZU-KUBERNETES-CLUSTER-NAME-ca`, consulte Obtener los secretos del clúster de Tanzu Kubernetes.

Comprobar la compatibilidad del clúster de Tanzu Kubernetes para actualizar

Una versión de Tanzu Kubernetes proporciona la distribución de software de Kubernetes firmada y compatible con VMware para los clústeres de Tanzu Kubernetes que aprovisiona servicio Tanzu Kubernetes Grid.

Notas de la versión de versiones de Tanzu Kubernetes

Para obtener una lista de todas las versiones de Tanzu Kubernetes, consulte las notas de la versión.

Comprobar la compatibilidad del clúster de Tanzu Kubernetes para actualizar

Antes de actualizar la infraestructura de vSphere with Tanzu, incluidos vCenter Server y clúster supervisor, consulte el artículo https://kb.vmware.com/s/article/82592 de la base de conocimientos para obtener instrucciones sobre cómo comprobar si algún clúster de Tanzu Kubernetes es incompatible con la actualización. Si un clúster de Tanzu Kubernetes no es compatible con la infraestructura de destino, actualice el clúster antes de continuar con la actualización del sistema.

Usar Kubectl para enumerar las versiones de Tanzu Kubernetes disponibles

Puede enumerar las versiones de Tanzu Kubernetes y ver la compatibilidad y la capacidad de actualización de cada versión con el siguiente comando.

```
kubectl get tanzukubernetesreleases
```

La columna COMPATIBLE indica si esa versión de Tanzu Kubernetes es compatible con el clúster supervisor actual. La columna UPDATES AVAILABLE indica si hay una actualización de Kubernetes disponible y la siguiente versiones de Tanzu Kubernetes recomendada que se utilizará.

```
NAME                                VERSION                            READY   COMPATIBLE
CREATED   UPDATES AVAILABLE
v1.18.15---vmware.1-tkg.1.600e412   1.18.15+vmware.1-tkg.1.600e412   True    True
21h       [1.19.7+vmware.1-tkg.1.fc82c41]
v1.19.7---vmware.1-tkg.1.fc82c41    1.19.7+vmware.1-tkg.1.fc82c41    True    True
21h       [1.20.2+vmware.1-tkg.1.1d4f79a]
v1.20.2---vmware.1-tkg.1.1d4f79a    1.20.2+vmware.1-tkg.1.1d4f79a    True    True         21h
```

Esta misma información también está disponible en kubectl get tkc <tkgs-cluster-name>.

Actualizar clústeres de Tanzu Kubernetes

Puede iniciar una actualización gradual de un clúster de Tanzu Kubernetes, incluida la versión de Kubernetes, mediante la actualización de la versión de Tanzu Kubernetes, la clase de máquina virtual o la clase de almacenamiento.

Lista de comprobación de preparación para la actualización de un clúster de Tanzu Kubernetes

Complete la siguiente lista de tareas de requisitos previos antes de realizar la actualización de un clúster de Tanzu Kubernetes.

Paso	Acción
1	Lea las vSphere with Tanzunotas de la versión.
2	Lea las versiones de Tanzu Kubernetesnotas de la versión.
3	Revise el vSphere with Tanzu Acerca de las actualizaciones de vSphere with Tanzu.
4	Compruebe la Tanzu Kubernetes Comprobar la compatibilidad del clúster de Tanzu Kubernetes para actualizar con las versiones de actualización de destino.
5	Revise las funciones de la versión de destino de la API de servicio Tanzu Kubernetes Grid, como Aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS, y la versión actual, como Aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha1 de servicio Tanzu Kubernetes Grid. (Consulte la nota importante más abajo).
6	Compruebe que todos los clústeres de Tanzu Kubernetes aprovisionados estén en un estado de Ver el estado del ciclo de vida de los clústeres de Tanzu Kubernetes.
7	Realice una Actualizar clúster supervisor mediante una actualización de los espacios de nombres de vSphere de espacios de nombres de vSphere que actualice el clúster supervisor y el servicio Tanzu Kubernetes Grid.

Paso	Acción
8	Revise las opciones para Iniciar una actualización gradual de un clúster de Tanzu Kubernetes de un clúster de Tanzu Kubernetes.
9	Revise los métodos Métodos para editar el manifiesto del clúster para actualizar el manifiesto del clúster.

Importante vSphere with Tanzu versión 7 Update 3, específicamente el clúster supervisor versión `v1.21.0+vmware.wcp.2`, incluye una actualización automática a la API v1alpha2 de servicio Tanzu Kubernetes Grid. Algunos campos de la especificación del clúster de Tanzu Kubernetes están obsoletos y es posible que el manifiesto del clúster deba editarse manualmente antes de actualizar la versión de Kubernetes. Consulte Actualizar una versión de Tanzu Kubernetes después de convertir la especificación del clúster a la API v1alpha2 de TKGS.

Iniciar una actualización gradual de un clúster de Tanzu Kubernetes

Para iniciar una actualización gradual, realice una o varias de las siguientes modificaciones en la especificación de `TanzuKubernetesCluster`:

- Actualizar un clúster de Tanzu Kubernetes mediante la actualización de la versión de Tanzu Kubernetes
- Actualizar un clúster de Tanzu Kubernetes mediante el cambio del objeto VirtualMachineClass
- Actualizar un clúster de Tanzu Kubernetes mediante el cambio de la clase de almacenamiento

Nota Si bien estas son las formas más comunes de iniciar una actualización gradual, no son las únicas. Un cambio en cualquiera de los elementos de configuración también puede iniciar una actualización gradual. Por ejemplo, si se cambia el nombre o se reemplaza el objeto `VirtualMachineImage` que corresponde a una versión de distribución, se inicia una actualización gradual, ya que el sistema intenta obtener todos los nodos que se ejecutan en la nueva imagen. Además, la actualización de clúster supervisor podrá activar una actualización gradual de los clústeres de Tanzu Kubernetes implementados allí. Por ejemplo, si se actualiza `vmware-system-tkg-controller-manager`, el sistema introduce nuevos valores en el generador de manifiestos, y la controladora inicia una actualización gradual para implementar esos valores.

Métodos para editar el manifiesto del clúster

Para actualizar un clúster, es necesario actualizar el manifiesto del clúster. Existen varias formas de hacerlo, entre ellas:

- Mediante el comando `kubectl edit tanzukubernetescluster/CLUSTER-NAME`. Este comando abre todo el manifiesto del clúster en el editor de texto definido por las variables de entorno KUBE_EDITOR o EDITOR. Al guardar el archivo, el clúster se actualiza con los cambios. Para obtener más información sobre el comando `kubectl edit`, consulte el comando de edición en la documentación de Kubernetes. Para utilizar el método `kubectl edit`, consulte los siguientes temas:
  - Actualizar un clúster de Tanzu Kubernetes mediante la actualización de la versión de Tanzu Kubernetes
  - Actualizar un clúster de Tanzu Kubernetes mediante el cambio del objeto VirtualMachineClass
  - Actualizar un clúster de Tanzu Kubernetes mediante el cambio de la clase de almacenamiento
- Mediante el comando `kubectl patch`. Este comando realiza una actualización "in situ" de un clúster. El propósito de este comando consiste en proporcionar un método para actualizar las versiones de Kubernetes y es el enfoque que se explica aquí. Para obtener más información sobre el comando `kubectl patch`, consulte Actualizar los objetos de la API mediante la revisión de kubectl en la documentación de Kubernetes. Para utilizar el método `kubectl patch`, consulte el siguiente tema:
  - Actualizar los clústeres de Tanzu Kubernetes con el método de revisión
- Mediante el comando `kubectl apply` con un archivo YAML local que se actualiza manualmente. Si bien este enfoque tiene la ventaja de ser similar al proceso de Flujo de trabajo para aprovisionar clústeres de Tanzu Kubernetes mediante la API v1alpha2 de TKGS, si no tiene acceso al YAML del clúster actual, el enfoque puede ser destructivo y, por lo tanto, no se recomienda.

Actualizar un clúster de Tanzu Kubernetes mediante la actualización de la versión de Tanzu Kubernetes

Actualice un clúster de Tanzu Kubernetes mediante la actualización de la versión de versión de Tanzu Kubernetes.

Puede iniciar una actualización gradual de un clúster de Tanzu Kubernetes mediante la actualización de la versión de versión de Tanzu Kubernetes. La forma de hacerlo varía según la versión de la API de servicio Tanzu Kubernetes Grid que esté utilizando.

Versión de API de TKGS	Método de actualización de la versión
API v1alpha2	Actualice la cadena TKR NAME en las propiedades `spec.topology.controlPlane.tkr.refernece.name` y `spec.topology.nodePools[*].tkr.reference.name` del manifiesto del clúster. Consulte Actualizar una versión de Tanzu Kubernetes después de convertir la especificación del clúster a la API v1alpha2 de TKGS.
API v1alpha1	Actualice la versión de DISTRIBUCIÓN en las propiedades `spec.distribution.version` y `spec.distribution.fullVersion` del manifiesto del clúster. Ver a continuación

Requisitos previos

Verifique la finalización de los requisitos previos para actualizar los clústeres de Tanzu Kubernetes. Consulte Actualizar clústeres de Tanzu Kubernetes.

Esta tarea utiliza el comando `kubectl edit tanzukubernetescluster/CLUSTER-NAME` para actualizar el manifiesto del clúster. El comando kubectl edit abre el manifiesto del clúster en el editor de texto definido por las variables de entorno KUBE_EDITOR o EDITOR. Al guardar el archivo, el clúster se actualiza con los cambios. Consulte Especificar un editor de texto predeterminado para Kubectl.

Procedimiento

1 Realice la autenticación con clúster supervisor. Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

```
kubectl vsphere login --server=IP-ADDRESS --vsphere-username USERNAME
```

2 Cambie el contexto al espacio de nombres de vSphere donde se aprovisiona el clúster de Tanzu Kubernetes de destino.

```
kubectl config use-context SUPERVISOR-NAMESPACE
```

3 Obtenga la versión y el clúster de Tanzu Kubernetes de destino.

```
kubectl get tanzukubernetescluster
```

Por ejemplo, el resultado con la API v1alpha2 de TKGS:

```
kubectl get tanzukubernetescluster
NAMESPACE         NAME            CONTROL PLANE   WORKER   TKR
NAME                              AGE    READY    TKR COMPATIBLE   UPDATES AVAILABLE
tkgs-cluster-1    test-cluster    3               3        v1.21.2---vmware.1-
tkg.1.ee25d55      38h    True    True              [1.21.2+vmware.1-tkg.1.ee25d55]
```

Por ejemplo, el resultado con la API v1alpha1 de TKGS :

```
kubectl get tanzukubernetescluster
NAME              CONTROL PLANE   WORKER   DISTRIBUTION                      AGE   PHASE
tkgs-cluster-1    3               3        v1.19.16+vmware.1-tkg.1.df910e2   19h   running
```

4 Enumere las versiones disponibles de Tanzu Kubernetes.

```
kubectl get tanzukubernetesreleases
```

5 Ejecute el siguiente comando para editar el manifiesto del clúster.

```
kubectl edit tanzukubernetescluster/CLUSTER-NAME
```

6 Edite el manifiesto actualizando versión de Tanzu Kubernetes. La forma de hacerlo varía según la versión de la API TKGS que esté utilizando.

Si utiliza la API v1alpha2 de TKGS, actualice la cadena TKR NAME. Consulte Actualizar una versión de Tanzu Kubernetes después de convertir la especificación del clúster a la API v1alpha2 de TKGS.

Si utiliza la API v1alpha1 de TKGS, actualice el manifiesto desde, por ejemplo:

```
spec:
  distribution:
    fullVersion: v1.19.16+vmware.1-tkg.1.df910e2
    version: v1.19.16
```

Para, por ejemplo:

```
spec:
  distribution:
    fullVersion: null
    version: v1.20.12
```

Nota Si utiliza la API v1alpha1 de TKGS, puede especificar la versión completa o utilizar un acceso directo a la versión, como `version: v1.20.12`, que se resuelve en la imagen más reciente que coincide con esa versión de revisión, o `version: v1.20`, que se resuelve. a la versión de revisión coincidente más reciente. La versión resuelta se muestra como `fullVersion` en el manifiesto del clúster. Para realizar una actualización de versión mediante un acceso directo, debe anular la configuración de `fullVersion` para evitar una posible falta de coincidencia de versiones durante la detección.

7 Guarde los cambios que hizo en el archivo de manifiesto.

Cuando guarde el archivo, kubectl aplicará los cambios al clúster. En segundo plano, el servicio de máquina virtual en el clúster supervisor aprovisiona el nuevo nodo de trabajo.

8 Compruebe que kubectl notifique el correcto registro de los cambios en el manifiesto.

```
kubectl edit tanzukubernetescluster/tkgs-cluster-1
tanzukubernetescluster.run.tanzu.vmware.com/tkgs-cluster-1 edited
```

Nota Si recibe un error, o kubectl no informa de que el manifiesto del clúster se editó correctamente, asegúrese de haber configurado bien el editor de texto predeterminado con la variable de entorno KUBE_EDITOR. Consulte Especificar un editor de texto predeterminado para Kubectl.

9 Compruebe que el clúster se esté actualizando.

```
kubectl get tanzukubernetescluster
NAME             CONTROL PLANE   WORKER   DISTRIBUTION                       AGE   PHASE
tkgs-cluster-1   3               3        v1.20.12+vmware.1-tkg.1.b9a42f3   21h   updating
```

10 Compruebe que el clúster se haya actualizado.

```
kubectl get tanzukubernetescluster
NAME             CONTROL PLANE   WORKER   DISTRIBUTION                       AGE   PHASE
tkgs-cluster-1   3               3        v1.20.12+vmware.1-tkg.1.b9a42f3    22h   running
```

Actualizar un clúster de Tanzu Kubernetes mediante el cambio del objeto VirtualMachineClass

Puede actualizar un clúster de Tanzu Kubernetes si cambia la clase de máquina virtual que se utiliza para alojar los nodos del clúster.

servicio Tanzu Kubernetes Grid admite la actualización de un clúster cambiando la definición de `VirtualMachineClass`. Si lo hace, el servicio implementa gradualmente los nodos nuevos con esa nueva clase y reduce la velocidad de los nodos antiguos. Consulte Acerca de las actualizaciones de clústeres de servicio Tanzu Kubernetes Grid.

Nota La `VirtualMachineClass` debe estar enlazada al espacio de nombres de vSphere donde se aprovisiona el clúster de Tanzu Kubernetes. Consulte Clases de máquina virtual para clústeres de Tanzu Kubernetes.

Requisitos previos

Esta tarea utiliza el comando `kubectl edit tanzukubernetescluster/CLUSTER-NAME` para actualizar el manifiesto del clúster. El comando kubectl edit abre el manifiesto del clúster en el editor de texto definido por las variables de entorno KUBE_EDITOR o EDITOR. Al guardar el archivo, el clúster se actualiza con los cambios. Consulte Especificar un editor de texto predeterminado para Kubectl.

Procedimiento

1 Realice la autenticación con clúster supervisor. Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

```
kubectl vsphere login --server=IP-ADDRESS --vsphere-username USERNAME
```

2 Cambie el contexto al espacio de nombres de vSphere donde se aprovisiona el clúster de Tanzu Kubernetes de destino.

```
kubectl config use-context SUPERVISOR-NAMESPACE
```

3 Describa el clúster de Tanzu Kubernetes de destino y compruebe la clase de máquina virtual.

```
kubectl describe tanzukubernetescluster CLUSTER-NAME
```

Por ejemplo, este clúster utiliza la clase de máquina virtual best-effort-medium:

```
Spec:
  ...
  Topology:
    Control Plane:
      Class:          best-effort-medium
      ...
    Workers:
      Class:          best-effort-medium
      ...
```

4 Enumere y describa las clases de máquina virtual disponibles en el espacio de nombres.

```
kubectl get virtualmachineclassbindings
```

Nota El comando `kubectl get virtualmachineclasses` enumera todas las clases de máquina virtual presentes en el clúster supervisor. Debido a que debe asociar las clases de máquina virtual con el espacio de nombres de vSphere, solo puede usar las clases de máquina virtual que están enlazadas al espacio de nombres de destino.

5 Ejecute el siguiente comando para editar el manifiesto del clúster.

```
kubectl edit tanzukubernetescluster/CLUSTER-NAME
```

6 Puede editar el manifiesto si cambia la cadena de `version` y desactiva o anula `fullVersion` para evitar un posible error de coincidencia de versiones durante la detección.

Por ejemplo, cambie el uso de la clase de máquina virtual `best-effort-medium` en el manifiesto del clúster para los nodos de trabajo y el plano de control:

```
spec:
  topology:
```

```
    controlPlane:
      class: best-effort-medium
      ...
    workers:
      class: best-effort-medium
      ...
```

Para usar la clase de máquina virtual `guaranteed-large` para los nodos de trabajo y el plano de control:

```
spec:
  topology:
    controlPlane:
      class: guaranteed-large
      ...
    workers:
      class: guaranteed-large
      ...
```

7 Guarde los cambios que hizo en el archivo de manifiesto.

Cuando guarde el archivo, kubectl aplicará los cambios al clúster. En segundo plano, servicio Tanzu Kubernetes Grid aprovisiona las máquinas virtuales del nuevo nodo y reduce la velocidad de las antiguas.

8 Compruebe que kubectl notifique el correcto registro de los cambios en el manifiesto.

```
kubectl edit tanzukubernetescluster/tkgs-cluster-1
tanzukubernetescluster.run.tanzu.vmware.com/tkgs-cluster-1 edited
```

Nota Si recibe un error, o kubectl no informa de que el manifiesto del clúster se editó correctamente, asegúrese de haber configurado bien el editor de texto predeterminado con la variable de entorno KUBE_EDITOR. Consulte Especificar un editor de texto predeterminado para Kubectl.

9 Compruebe que el clúster se esté actualizando.

```
kubectl get tanzukubernetescluster
NAME             CONTROL PLANE   WORKER   DISTRIBUTION                     AGE   PHASE
tkgs-cluster-1   3               3        v1.18.5+vmware.1-tkg.1.c40d30d   21h   updating
```

10 Compruebe que el clúster se haya actualizado.

```
kubectl get tanzukubernetescluster
NAME             CONTROL PLANE   WORKER   DISTRIBUTION                     AGE   PHASE
tkgs-cluster-1   3               3        v1.18.5+vmware.1-tkg.1.c40d30d   22h   running
```

Actualizar un clúster de Tanzu Kubernetes mediante el cambio de la clase de almacenamiento

Puede actualizar un clúster de Tanzu Kubernetes si cambia la clase de almacenamiento que utilizan los nodos del clúster.

servicio Tanzu Kubernetes Grid admite la actualización de un clúster cambiando el objeto `StorageClass` de los grupos de nodos, es decir, si cambia la propiedad `.spec.topology.controlPlane.storageClass` o `.spec.topology.workers.storageClass`. Consulte Acerca de las actualizaciones de clústeres de servicio Tanzu Kubernetes Grid.

Requisitos previos

Esta tarea utiliza el comando `kubectl edit tanzukubernetescluster/CLUSTER-NAME` para actualizar el manifiesto del clúster. El comando kubectl edit abre el manifiesto del clúster en el editor de texto definido por las variables de entorno KUBE_EDITOR o EDITOR. Al guardar el archivo, el clúster se actualiza con los cambios. Consulte Especificar un editor de texto predeterminado para Kubectl.

Procedimiento

1 Realice la autenticación con clúster supervisor. Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

```
kubectl vsphere login --server=IP-ADDRESS --vsphere-username USERNAME
```

2 Cambie el contexto al espacio de nombres de vSphere donde se aprovisiona el clúster de Tanzu Kubernetes de destino.

```
kubectl config use-context SUPERVISOR-NAMESPACE
```

3 Para determinar las clases de almacenamiento disponibles y decidir cuál debe usar, ejecute el siguiente comando.

```
kubectl describe tanzukubernetescluster CLUSTER-NAME
```

4 Ejecute el siguiente comando para editar el manifiesto del clúster.

```
kubectl edit tanzukubernetescluster/CLUSTER-NAME
```

5 Edite el manifiesto cambiando el valor de `storageClass`.

Por ejemplo, cambie el manifiesto del clúster de la clase `silver-storage-class` para los nodos de trabajo y el plano de control:

```
spec:
  topology:
    controlPlane:
      ...
```

```
      storageClass: silver-storage-class
    workers:
      ...
      storageClass: silver-storage-class
```

Si desea usar la clase `gold-storage-class` para los nodos de trabajo y el plano de control:

```
spec:
  topology:
    controlPlane:
      ...
      storageClass: gold-storage-class
    workers:
      ...
      storageClass: gold-storage-class
```

6 Guarde los cambios que hizo en el archivo de manifiesto.

Cuando guarde el archivo, kubectl aplicará los cambios al clúster. En segundo plano, servicio Tanzu Kubernetes Grid aprovisiona las máquinas virtuales del nuevo nodo y reduce la velocidad de las antiguas.

7 Compruebe que kubectl notifique el correcto registro de los cambios en el manifiesto.

```
kubectl edit tanzukubernetescluster/tkgs-cluster-1
tanzukubernetescluster.run.tanzu.vmware.com/tkgs-cluster-1 edited
```

Nota Si recibe un error, o kubectl no informa de que el manifiesto del clúster se editó correctamente, asegúrese de haber configurado bien el editor de texto predeterminado con la variable de entorno KUBE_EDITOR. Consulte Especificar un editor de texto predeterminado para Kubectl.

8 Compruebe que el clúster se esté actualizando.

```
kubectl get tanzukubernetescluster
NAME             CONTROL PLANE   WORKER   DISTRIBUTION                       AGE   PHASE
tkgs-cluster-1   3               3        v1.18.5+vmware.1-tkg.1.c40d30d     21h   updating
```

9 Compruebe que el clúster se haya actualizado.

```
kubectl get tanzukubernetescluster
NAME             CONTROL PLANE   WORKER   DISTRIBUTION                       AGE   PHASE
tkgs-cluster-1   3               3        v1.18.5+vmware.1-tkg.1.c40d30d     22h   running
```

Actualizar los clústeres de Tanzu Kubernetes con el método de revisión

Puede utilizar el método `kubectl patch` para realizar una actualización "in situ" de un clúster de Tanzu Kubernetes. El método `kubectl patch` es una alternativa al uso del comando `kubectl edit` para realizar una de las operaciones de actualización del clúster compatibles.

Acerca del comando Kubectl Patch

Restricción No intente utilizar `kubectl patch` como se describe en este tema para actualizar una especificación de clúster para que cumpla con la API v1alpha2 de TKGS. Para este tipo de actualización, debe utilizar `kubectl edit`. Consulte Actualizar una versión de Tanzu Kubernetes después de convertir la especificación del clúster a la API v1alpha2 de TKGS.

El comando `kubectl patch` realiza una actualización "in situ" de un clúster. El propósito de este comando consiste en proporcionar un método para actualizar las versiones de Kubernetes y es el enfoque que se explica aquí. Para obtener más información sobre el comando `kubectl patch`, consulte Actualizar los objetos de la API mediante la revisión de kubectl en la documentación de Kubernetes.

El método que se demuestra aquí utiliza el comando de Shell de UNIX `read` para tomar la entrada del teclado y asignarla a una variable denominada `$PATCH`. El comando `kubectl patch` invoca a la API de Kubernetes para actualizar el manifiesto del clúster. La marca `--type=merge` indica que los datos contienen solo las propiedades que son diferentes del manifiesto existente.

Actualizar la versión de Kubernetes con el método de revisión

El método más común para activar una actualización gradual es cambiar la versión de distribución de Kubernetes del clúster, mediante la propiedad `.spec.distribution.version` o `.spec.distribution.fullVersion`. Actualice la sugerencia de `version` y desactive o anule `fullVersion` para evitar que se produzca un error de coincidencia de versiones durante la detección.

```
$ read -r -d '' PATCH <<'EOF'
spec:
  distribution:
    fullVersion: null    # NOTE: Must set to null when updating just the version field
    version: v1.18.5
EOF
```

Aplique la actualización mediante el comando `kubectl patch`. Debe incluir las comillas alrededor de la variable `"$PATCH"` para conservar los caracteres de línea nueva en el manifiesto del clúster. Reemplace el valor *TKG-CLUSTER-NAME* por el nombre real del clúster.

```
kubectl patch --type=merge tanzukubernetescluster TKG-CLUSTER-NAME --patch "$PATCH"
```

Resultado esperado:

```
tanzukubernetescluster.run.tanzu.vmware.com/TKG-CLUSTER-NAME patched
```

Actualizar el clúster mediante el cambio del objeto VirtualMachineClass para los nodos con el método de revisión

Otra forma de activar una actualización gradual de un clúster de Tanzu Kubernetes es cambiar el objeto `VirtualMachineClass` de los grupos de nodos, es decir, cambiar las propiedades `.spec.topology.controlPlane.class` o `.spec.topology.workers.class`.

```
read -r -d '' PATCH <<'EOF'
spec:
  topology:
    controlPlane:
      class: best-effort-xlarge
    workers:
      class: best-effort-xlarge
EOF
```

Aplique la actualización mediante el comando `kubectl patch` y reemplace la variable por el nombre del clúster.

```
kubectl patch --type=merge tanzukubernetescluster TKG-CLUSTER-NAME --patch "$PATCH"
```

Resultado esperado:

```
tanzukubernetescluster.run.tanzu.vmware.com/TKG-CLUSTER-NAME patched
```

Actualizar el clúster mediante el cambio del objeto StorageClass para los nodos con el método de revisión

Otra forma de activar una actualización gradual de un clúster de Tanzu Kubernetes es cambiar el objeto `StorageClass` de los grupos de nodos, es decir, cambiar las propiedades `.spec.topology.controlPlane.storageClass` o `.spec.topology.workers.storageClass`.

```
$ read -r -d '' PATCH <<'EOF'
spec:
  topology:
    controlPlane:
      storageClass: gc-storage-profile
    workers:
      storageClass: gc-storage-profile
EOF
```

Aplique la actualización mediante el comando `kubectl patch` y reemplace la variable por el nombre del clúster.

```
kubectl patch --type=merge tanzukubernetescluster TKG-CLUSTER-NAME --patch "$PATCH"
```

Resultado esperado:

```
tanzukubernetescluster.run.tanzu.vmware.com/TKG-CLUSTER-NAME patched
```

Copia de seguridad y restauración de vSphere with Tanzu 18

Puede realizar una copia de seguridad y restaurar las cargas de trabajo que se ejecutan en los clústeres de pods de vSphere y Tanzu Kubernetes, así como la infraestructura de vCenter Server y NSX-T que respalda su instalación de vSphere with Tanzu.

Este capítulo incluye los siguientes temas:

- Consideraciones para realizar copias de seguridad y restaurar vSphere with Tanzu
- Instalar y configurar el complemento de Velero para vSphere en el clúster supervisor
- Realizar copias de seguridad y restaurar pods de vSphere mediante el complemento complemento de Velero para vSphere
- Instalar y configurar el complemento de Velero para vSphere en un clúster de Tanzu Kubernetes
- Copia de seguridad y restauración de cargas de trabajo del clúster de Tanzu Kubernetes mediante complemento de Velero para vSphere
- Instalar y configurar Velero y Restic independientes en un clúster de Tanzu Kubernetes
- Copia de seguridad y restauración de cargas de trabajo de clúster de Tanzu Kubernetes mediante Restic y Velero independientes
- Copia de seguridad y restauración de vCenter Server
- Copia de seguridad y restauración de NSX-T Data Center

Consideraciones para realizar copias de seguridad y restaurar vSphere with Tanzu

Este tema proporciona una descripción general del proceso de copia de seguridad y restauración de vSphere with Tanzu, y proporciona consideraciones de alto nivel para implementar la estrategia de copia de seguridad y restauración de vSphere with Tanzu.

La copia de seguridad y la restauración de vSphere with Tanzu constan de varias capas y herramientas.

La tabla resume estas capas y herramientas desde la carga de trabajo de arriba hacia abajo hasta la infraestructura. Consulte las secciones individuales para obtener detalles sobre cómo realizar la copia de seguridad y la restauración de esa capa.

Situación	Tools	Comentarios
Copia de seguridad y restauración de pods de vSphere	Complemento de Velero para vSphere	Instale y configure el complemento en el clúster supervisor. **Nota** El complemento no está realizando una copia de seguridad del estado del clúster supervisor. Consulte Instalar y configurar el complemento de Velero para vSphere en el clúster supervisor. Consulte Realizar copias de seguridad y restaurar pods de vSphere mediante el complemento complemento de Velero para vSphere.
Copia de seguridad de cargas de trabajo sin estado y con estado en un clúster de Tanzu Kubernetes y restauración en un clúster aprovisionado por Tanzu Kubernetes Grid Service	Complemento de Velero para vSphere	Se puede realizar una copia de seguridad y restaurar tanto los metadatos de Kubernetes como los volúmenes persistentes. La creación de instantáneas de Velero (no Restic) se utiliza para los volúmenes persistentes. Consulte Instalar y configurar el complemento de Velero para vSphere en un clúster de Tanzu Kubernetes. Consulte Copia de seguridad y restauración de cargas de trabajo del clúster de Tanzu Kubernetes mediante complemento de Velero para vSphere.
Copia de seguridad de cargas de trabajo sin estado y con estado en un clúster de Tanzu Kubernetes y restauración en un clúster de Kubernetes conforme no aprovisionado por Tanzu Kubernetes Grid Service	Restic y Velero independientes	Si necesita portabilidad, utilice Velero independiente. Debe incluir Restic para las aplicaciones con estado. Consulte Instalar y configurar Velero y Restic independientes en un clúster de Tanzu Kubernetes. Consulte Copia de seguridad y restauración de cargas de trabajo de clúster de Tanzu Kubernetes mediante Restic y Velero independientes.
Clúster supervisor Después de actualizar un clúster supervisor, debe realizar una nueva copia de seguridad. No se permite restaurar una instancia de vCenter Server en una copia de seguridad en la que se espera una versión anterior del clúster supervisor.	vCenter Server Complemento de Velero para vSphere Restic y Velero independientes	Restaure vCenter Server desde la copia de seguridad. vCenter volverá a crear las tres máquinas virtuales del plano de control del clúster supervisor. Restaure las cargas de trabajo del clúster a partir de una copia de seguridad mediante el complemento o Velero y Restic independientes.

Situación	Tools	Comentarios
Configuración de vCenter	vCenter Server	Si se pierde vCenter, utilice vCenter Server para realizar una copia de seguridad y restaurar los objetos de vCenter. Consulte Copia de seguridad y restauración de vCenter Server.
NSX-T Data Center	NSX-T Manager	El equilibrador de carga y los servicios de entrada dependen de la copia de seguridad de NSX-T. Utilice NSX-T Manager para realizar una copia de seguridad y restaurar la base de datos de NSX-T. Consulte Copia de seguridad y restauración de NSX-T Data Center.

Instalar y configurar el complemento de Velero para vSphere en el clúster supervisor

Puede utilizar el complemento de Velero para vSphere para realizar copias de seguridad y restauración de cargas de trabajo que se ejecutan en pods de vSphere mediante la instalación del complemento de Velero para vSphere en el clúster supervisor.

Descripción general

El complemento de Velero para vSphere proporciona una solución para hacer copias de seguridad y restauración de cargas de trabajo de vSphere with Tanzu. La solución requiere la instalación y configuración de varios componentes. Una vez que haya instalado y configurado el complemento de Velero para vSphere en el clúster supervisor, puede realizar copias de seguridad y restauración de pods de vSphere. Para cargas de trabajo persistentes, el complemento de Velero para vSphere le permite tomar instantáneas de los volúmenes persistentes.

La instalación del complemento de Velero para vSphere en el clúster supervisor también es un requisito previo para usar el complemento de Velero para vSphere para realizar una copia de seguridad y restauración de cargas de trabajo del clúster de Tanzu Kubernetes.

Nota El complemento de Velero para vSphere no se puede utilizar para realizar copias de seguridad y restauración del estado del clúster supervisor. Consulte Consideraciones para realizar copias de seguridad y restaurar vSphere with Tanzu.

Nota El complemento de Velero para vSphere por sí mismo no realiza copias de seguridad incrementales. Dell EMC PowerProtect admite copias de seguridad incrementales y aprovecha Velero y el complemento de Velero para vSphere.

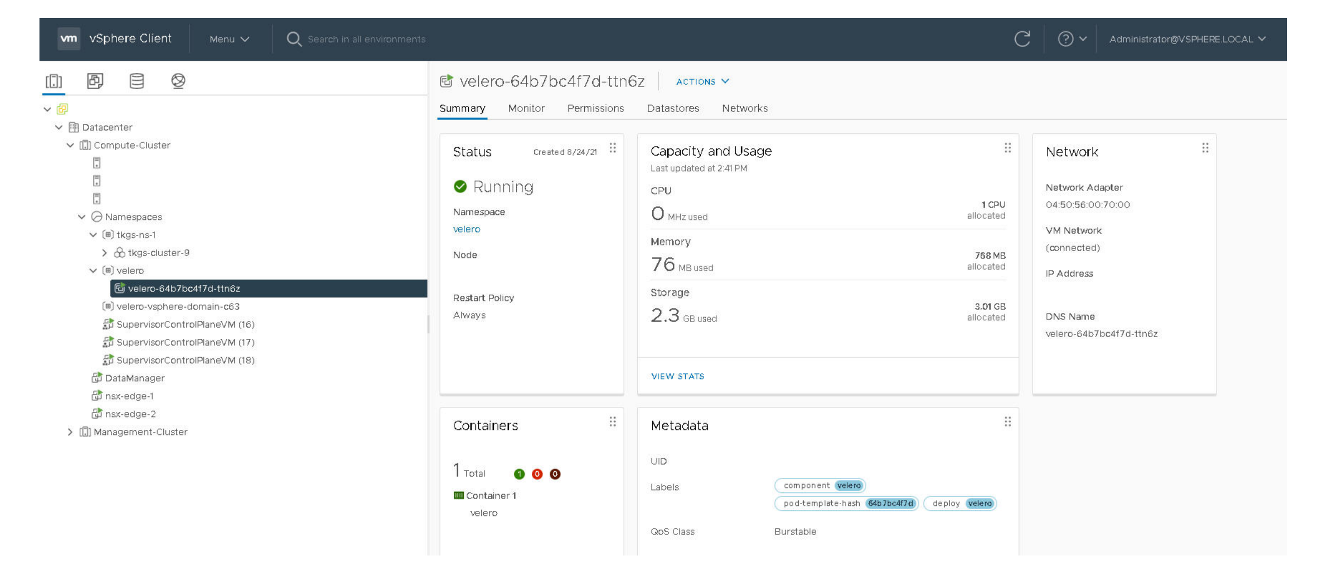
Requisitos previos

Antes de instalar el complemento de Velero para vSphere, cumpla con los siguientes requisitos previos:

- La Administración de cargas de trabajo está habilitada con redes de NSX-T Data Center. Consulte Habilitar la administración de cargas de trabajo con redes de NSX-T Data Center.
- El clúster supervisor es versión 1.21.1 o posterior.
- Se crea y se configura el espacio de nombres de vSphere.
- Debe ser miembro de la función de administrador de vSphere o tener los siguientes privilegios de vSphere:
  - **SupervisorServices.Manage**
  - **Namespaces.Manage**
  - **Namespaces.Configure**

La captura de pantalla muestra el estado final de una instalación de complemento de Velero para vSphere.

- Las redes de NSX-T se utilizan para admitir la implementación de pods de vSphere
- Se implementa una máquina virtual de Data Manager
- El operador Velero está habilitado y en ejecución en el espacio de nombres `velero-vsphere-domain-cXX`
- Se configura un espacio de nombres denominado `velero`
- El complemento de Velero para vSphere se ejecuta como un pod de vSphere en el espacio de nombres `velero`



Actualizaciones

Estas instrucciones asumen que está ejecutando vSphere 7 U3. Si instaló previamente el complemento de Velero para vSphere en un entorno vSphere 7 U2 P3, al actualizar, la máquina virtual de Data Manager y **Velero vSphere Operator** se migrarán al nuevo marco. **Velero vSphere Operator** se convierte al nuevo formato de servicios de vSphere. No es necesaria ninguna acción.

Crear una red dedicada para el tráfico de copia de seguridad y restauración (opcional)

Aunque no es necesario, se recomienda que, para los entornos de producción, separe el tráfico de copia de seguridad y restauración del tráfico de red de administración de vSphere with Tanzu. Existen dos aspectos que se deben considerar sobre esto:

- Etiquete los hosts ESXi para admitir la copia de archivo de red (Network File Copy, NFC)
- Configure la red de copia de seguridad y restauración mediante NSX-T Data Center

Para configurar hosts ESXi de vSphere 7.x de modo que admitan un transporte de dispositivo de bloques de red (Network Block Device, NBD) dedicado, agregue una NIC de VMkernel en cada host ESXi del clúster de vCenter Server en el que esté habilitada Administración de cargas de trabajo y establezca `vSphereBackupNFC` en esa NIC. Cuando se aplica la etiqueta `vSphereBackupNFC` al tipo de NIC para un adaptador de VMkernel, el tráfico de copia de seguridad y restauración pasa por la NIC virtual elegida.

Para realizar esta configuración, utilice Virtual Disk Development Kit. Consulte la documentación del NBD.

Nota Si la `vSphereBackupNFC` no está habilitada en la NIC de VMkernel, el tráfico de copia de seguridad y restauración no se enviará a la red de copia de seguridad y restauración, aunque configure una. Si no se habilita `vSphereBackupNFC`, el tráfico viajará por la red de administración de vSphere.

Una vez habilitada la etiqueta de `vSphereBackupNFC`, configure la red de copia de seguridad y restauración mediante NSX-T; para ello, actualice el conmutador distribuido de vSphere (vSphere Distributed Switch, vDS) existente para el clúster de la siguiente manera:

- En vSphere Client, seleccione **Menú > Redes**.
- Seleccione el vDS existente para el clúster.
- Haga clic con el botón secundario en el vDS y seleccione **Grupo de puertos distribuidos > Nuevo grupo de puertos distribuidos**.
- Cree un nuevo grupo de puertos distribuidos denominado **BackupRestoreNetwork**.
- Agregue un adaptador de VMkernel al grupo de puertos distribuidos **BackupRestoreNetwork**.
- Asocie todos los hosts ESXi del clúster de vCenter en el que la Administración de cargas de trabajo está habilitada al grupo de puertos distribuidos **BackupRestoreNetwork**.
- Habilite la etiqueta `vSphereBackupNFC`.

Para obtener instrucciones sobre cómo crear una red de NSX-T en el vDS existente, consulte Instalar y configurar NSX-T Data Center para vSphere with Tanzu.

Crear un almacén de objetos compatible con S3

Para realizar copias de seguridad y restauraciones de volúmenes persistentes, debe proporcionar un almacén de objetos compatible con S3. Velero admite varios proveedores de almacenes objetos.

Para instalar el complemento de Velero para vSphere, deberá proporcionar la siguiente información sobre el almacén de objetos compatible con S3:

Elemento de datos	Valor de ejemplo
s3Url	http://my-s3-store.example.com
aws_access_key_id	ACCESS-KEY-ID-STRING
aws_secret_access_key	SECRET-ACCESS-KEY-STRING

Cree un nombre de archivo de secretos `s3-credentials` con la siguiente información. Debe hacer referencia a este archivo cuando instale el complemento de Velero para vSphere.

```
[default]
aws_access_key_id = ACCESS-KEY-ID-STRING
aws_secret_access_key = SECRET-ACCESS-KEY-STRING
```

MinIO es un almacén de objetos compatible con S3 que es fácil de instalar y utilizar. vSphere with Tanzu se incluye con un servicio de supervisor de MinIO que puede habilitar. Para obtener más información, consulte Habilitar servicios con estado en vSphere with Tanzu.

Como alternativa, puede instalar manualmente un servidor MinIO en una máquina virtual Linux. Para obtener instrucciones, consulte Instalar y configurar Velero y Restic independientes en un clúster de Tanzu Kubernetes.

Instalar y configurar el administrador de datos

Para facilitar la copia de seguridad y la restauración mediante el complemento de Velero para vSphere, implemente una o varias máquinas virtuales de Data Manager para mover los datos de copia de seguridad de volúmenes persistentes dentro y fuera del almacenamiento de objetos compatible con S3. Data Manager mueve los datos de instantáneas de volumen desde el volumen de vSphere hasta el almacenamiento compatible con S3 remoto y durable en la copia de seguridad, y desde el almacenamiento compatible con S3 remoto hasta un volumen de vSphere durante la restauración.

En un entorno de vSphere with Tanzu, instale Data Manager como máquina virtual.

Nota No encienda la máquina virtual de Data Manager hasta que haya habilitado operador para vSphere de Velero.

1 Descargue el OVA de Data Manager:

https://vsphere-velero-datamgr.s3-us-west-1.amazonaws.com/datamgr-ob-17253392-photon-3-release-1.1.ova

2 Con vSphere Client, haga clic con el botón secundario en el **centro de datos** en el que está habilitada la Administración de cargas de trabajo y seleccione **Implementar plantilla de OVF**.

3 Seleccione el archivo OVA de Data Manager que descargó y cárguelo en el vCenter Server.

4 Asigne un nombre a la máquina virtual, como `DataManager`, por ejemplo.

5 Seleccione el recurso informático que es el clúster de vCenter en el que está configurado el clúster supervisor.

6 Revise los detalles de la implementación de la máquina virtual y haga clic en **Siguiente**.

7 Acepte los acuerdos de licencia y haga clic en **Siguiente**.

8 Seleccione el almacenamiento y haga clic en **Siguiente**.

9 Seleccione la red de destino para la máquina virtual de Data Manager.

   - Seleccione la **BackupRestoreNetwork** si configuró una red de copia de seguridad y restauración dedicada. Consulte Crear una red dedicada para el tráfico de copia de seguridad y restauración (opcional).
   - Seleccione la **red de administración** si no configuró una red de copia de seguridad y restauración dedicada.

10 Confirme las selecciones y haga clic en **Finalizar** para completar el proceso.

11 Utilice el panel Tareas recientes para supervisar el progreso de la implementación.

Nota Si recibe un error que indica "el descriptor de OVF no está disponible", utilice el navegador Chrome.

12 Una vez implementada la máquina virtual de Data Manager, configure los parámetros de entrada de la máquina virtual.

13 Haga clic con el botón secundario en la máquina virtual y seleccione **Editar configuración**.

14 En la pestaña Hardware virtual, para Unidad de CD/DVD, cambie de **Dispositivo host** a **Dispositivo cliente**.

Nota Si no lo hace, no podrá guardar las opciones de configuración avanzada requeridas.

15 En la pestaña **Editar configuración > Opciones de máquina virtual**, seleccione **Avanzado > Editar parámetros de configuración**.

16 Configure los parámetros de entrada para cada una de las siguientes opciones:

Parámetro	Valor
`guestinfo.cnsdp.vcUser`	Introduzca el nombre de usuario de vCenter Server con privilegios suficientes para implementar máquinas virtuales.
`guestinfo.cnsdp.vcAddress`	Introduzca la dirección IP o el FQDN de vCenter Server.
`guestinfo.cnsdp.vcPasswd`	Introduzca la contraseña de usuario vCenter Server.
`guestinfo.cnsdp.vcPort`	El valor predeterminado es **`443`**. No cambie este valor.
`guestinfo.cnsdp.wcpControlPlaneIP`	Introduzca la dirección IP del clúster supervisor. Para obtener este valor, desplácese hasta el clúster de vCenter donde está habilitada la Administración de cargas de trabajo y seleccione **Configurar > Espacios de nombres > Red > Red de administración > Dirección IP inicial**
`guestinfo.cnsdp.updateKubectl`	El valor predeterminado es **`false`**. No cambie este valor.
`guestinfo.cnsdp.veleroNamespace`	El valor predeterminado es **`velero`** y debe dejarlo así a menos que tenga una razón de peso para cambiarlo. Más adelante en el proceso, debe crear un espacio de nombres de vSphere en el clúster supervisor con el nombre `velero`. Estos nombres deben coincidir.
`guestinfo.cnsdp.datamgrImage`	Si no está configurado (sin configurar), el sistema extraerá de forma predeterminada la imagen de contenedor de Docker Hub en `vsphereveleroplugin/data-manager-for-plugin:1.1.0`

17 Haga clic en Aceptar para guardar la configuración y en Aceptar nuevamente para guardar la configuración de la máquina virtual.

Nota Si no cambió la unidad de CD/DVD de **Dispositivo host** a **Dispositivo cliente**, no podrá guardar la configuración. Si este es el caso, cancele la operación, cambie la unidad y repita los ajustes de configuración avanzada.

18 No encienda la máquina virtual de Data Manager hasta después de habilitar operador para vSphere de Velero (siguiente sección).

Instalar el servicio operador para vSphere de Velero en el clúster supervisor

vSphere with Tanzu proporciona operador para vSphere de Velero como un servicio de vSphere. El servicio operador para vSphere de Velero funciona con el complemento de Velero para vSphere para admitir la copia de seguridad y la restauración de cargas de trabajo de Kubernetes, incluida la creación de instantáneas de volúmenes persistentes. Para obtener más información sobre los servicios de vSphere, consulte Capítulo 8 Administrar servicios de supervisor con vSphere with Tanzu.

Complete la siguiente operación para registrar la especificación de **Velero vSphere Operator** con vCenter Server, donde **Administración de cargas de trabajo** está habilitada, y para instalar el **Velero vSphere Operator** como un servicio en el clúster supervisor.

Nota El **Velero vSphere Operator** se ejecuta como un pod de vSphere y requiere redes NSX-T.

---

1 Descargue el YAML de **Velero vSphere Operator** de la siguiente ubicación:

   http://vmware.com/go/supervisor-service

   El archivo de especificación de servicio se denomina `velero-supervisorservice-1.0.0.yaml`.

2 En el menú Inicio de vSphere Client, seleccione **Administración de cargas de trabajo**.

3 Seleccione la pestaña **Servicios**.

4 Seleccione la instancia de vCenter Server de destino en el menú desplegable de la parte superior.

5 Arrastre y suelte el archivo de especificación de servicio `velero-supervisorservice-1.0.0.yaml` que descargó en la tarjeta **Agregar nuevo servicio**.

   También puede hacer clic en **Agregar** y buscar y seleccionar el archivo `velero-supervisorservice-1.0.0.yaml`.

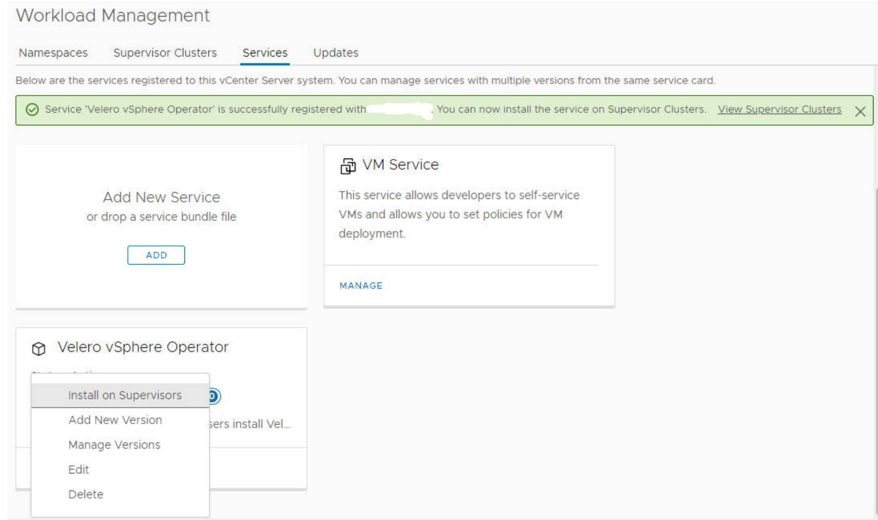
6 Haga clic en **Siguiente** y acepte el contrato de licencia.

7 Haga clic en **Finalizar**.

   El **Velero vSphere Operator** está registrado en vCenter Server. Compruebe que el servicio esté en un estado **Activo**. No puede instalar el servicio si está desactivado.

8 Busque la especificación de **Velero vSphere Operator** en la pestaña **Servicios**.

9 Haga clic en **Acciones > Instalar en supervisores**.



10 Seleccione el clúster supervisor de destino donde desea instalar el servicio.

Nota Si no ve su clúster supervisor, compruebe que esté utilizando redes NSX-T.

11 Configure el servicio **Velero vSphere Operator** de la siguiente manera:

   a Seleccione la versión en el menú desplegable: **1.1.0**.

   b No especifique un **Endpoint de repositorio**.

   c No introduzca un nombre de usuario o contraseña.

   d Haga clic en **Siguiente**.

12 Haga clic en **Finalizar** para completar la instalación del servicio.

Compruebe el servicio **Velero vSphere Operator** en el clúster supervisor e inicie la máquina virtual de Data Manager.

1 En el menú Inicio de vSphere Client, seleccione **Inventario**.

2 Seleccione el clúster de vCenter en el que está habilitada **Administración de cargas de trabajo**.

3 Seleccione **Configurar > Servicios de vSphere > Descripción general**.

4 Compruebe que puede ver que **Velero vSphere Operator** está instalado y que su estado es **Configurado**.

5 En el grupo de recursos **Espacios de nombres**, compruebe que ve un nuevo espacio de nombres denominado `svc-velero-vsphere-domain-xxx`, donde `xxx` es un token alfanumérico único. Este es el espacio de nombres que crea el sistema para **Velero vSphere Operator**.

Nota No es necesario configurar este espacio de nombres y no debe editarlo.

6 En la vista **Hosts y clústeres**, seleccione la máquina virtual de **Data Manager**.

7 Haga clic con el botón secundario en la máquina virtual de **Data Manager** y enciéndala.

Crear un espacio de nombres de vSphere para el complemento de Velero para vSphere

Con vSphere Client, cree manualmente un espacio de nombres de vSphere en el clúster supervisor. Este espacio de nombres es obligatorio para el complemento de Velero para vSphere. Para obtener instrucciones, consulte Creación y configuración de un espacio de nombres de vSphere.

- Denomine al espacio de nombres **`velero`**.
- Seleccione el espacio de nombres **velero** y configúrelo.
- Especifique el almacenamiento para el espacio de nombres **velero**.
- Otorgue a un usuario con los privilegios adecuados el permiso Editar en el espacio de nombres **velero**.

Instalar el complemento de Velero para vSphere

Ahora ya está listo para instalar el complemento de Velero para vSphere. Para ello, descargue y ejecute la CLI **velero-vsphere**.

Nota Este procedimiento requiere una máquina virtual Linux. Debe descargar y ejecutar **velero-vsphere** en el host de salto de Linux en el que ejecuta las CLI `kubectl-vsphere` y `kubectl`.

1 Cree una máquina virtual Linux donde pueda ejecutar la CLI. O bien, utilice un host de salto de Linux existente en el que acceda al clúster supervisor.

2 Descargue la CLI de complemento de Velero para vSphere desde la siguiente ubicación:

   https://github.com/vmware-tanzu/velero-plugin-for-vsphere/releases/download/v1.1.0/velero-vsphere-1.1.0-linux-amd64.tar.gz

3 Copie de forma segura la CLI en el host de salto de Linux. Por ejemplo:

```
pscp -P 22 C:\temp\velero-vsphere-1.1.0-linux-amd64.tar.gz ubuntu@10.117.29.131:/home/
ubuntu/tanzu
```

4 Extraiga la CLI `velero-vsphere` y haga que permita escritura.

```
tar -xf velero-vsphere-1.1.0-linux-amd64.tar.gz
chmod +x velero-vsphere
```

5 Cree el archivo `s3-credentials` con el siguiente contenido.

```
aws_access_key_id = ACCESS-KEY-ID-STRING
aws_secret_access_key = SECRET-ACCESS-KEY-STRING
```

6 Obtenga la región, la URL y el nombre del depósito para el almacén de objetos compatible con S3.

7 Inicie sesión en clúster supervisor mediante complemento de vSphere para kubectl.

8 Cambie el contexto al clúster supervisor.

```
kubectl config use-context SUPERVISOR-CLUSTER-IP-ADDRESS
```

9 Ejecute el siguiente comando de la CLI `velero-vsphere` para instalar el complemento de Velero para vSphere en el espacio de nombres **velero** que creó.

   Reemplace los valores de marcador de posición de los campos **`BUCKET-NAME`**, **`REGION`** (dos instancias) y **`s3Url`** con los valores adecuados. Si se desvió de cualquiera de las instrucciones anteriores, ajuste también esos valores, como el nombre o la ubicación del archivo de secretos, el nombre del espacio de nombres `velero` creado manualmente, etc.

```
./velero-vsphere install \
    --namespace velero \
    --image velero/velero:v1.5.1 \
```

```
    --provider aws \
    --plugins velero/velero-plugin-for-aws:v1.1.0,vsphereveleroplugin/velero-plugin-for-vsphere:1.1.0 \
    --bucket BUCKET-NAME \
    --secret-file s3-credentials \
    --snapshot-location-config region=REGION \
    --backup-location-config region=REGION,s3ForcePathStyle="true",s3Url=http://my-s3-store.example.com
```

Nota Puede utilizar complemento de Velero para vSphere v1.1.0 y versiones posteriores en el clúster supervisor, por ejemplo, `vsphereveleroplugin/velero-plugin-for-vsphere:v1.1.1` o `vsphereveleroplugin/velero-plugin-for-vsphere:v1.2.0`. La versión de Velero debe ser v1.5.1 (`velero/velero:v1.5.1`).

10 Compruebe que la instalación del complemento de Velero para vSphere se haya realizado correctamente.

Cuando la instalación se realiza correctamente, debería ver el siguiente mensaje:

```
Send the request to the operator about installing Velero in namespace velero
```

Ejecute el siguiente comando para realizar una verificación adicional. Debería ver "Completado" y la versión.

```
kubectl -n velero get veleroservice default -o json | jq '.status'
```

Resultado esperado:

```
{
  "enabled": true,
  "installphase": "Completed",
  "version": "v1.5.1"
}
```

Nota El comando anterior asume que tiene instalada la utilidad `jq`, que formatea la salida JSON enviada al terminal. Si no tiene `jq` instalada, instálela o elimine esa parte del comando (todo después de `json`).

11 Solucione problemas según sea necesario.

Si la instalación no se realiza correctamente, elimine la instalación e inténtelo de nuevo. Para eliminar la instalación, complete los pasos de la siguiente sección en el orden indicado.

Instalar el complemento de Velero en un entorno aislado

Si tiene pensado instalar el complemento de Velero para vSphere en un entorno aislado, debe hacerlo con imágenes personalizadas. Debe asegurarse de que las imágenes coincidentes de `backup-driver` y `data-manager-for-plugin` de las imágenes personalizadas estén disponibles en el registro esperado y que se pueda acceder a ellas desde el clúster de Kubernetes. En un entorno aislado, se esperan imágenes personalizadas del registro privado, ya que no es posible acceder a las imágenes publicadas en Docker Hub.

Para instalar el complemento, realice los siguientes pasos:

1. Descargue las imágenes publicadas de `velero-plugin-for-vsphere`, `backup-driver` y `data-manager-for-plugin`.
2. Cambie el nombre de las imágenes; es decir, etiquételas con los `<Registry endpoint and path>` y `<Version tag>` coincidentes y cárguelas en los repositorios personalizados.
3. Instale el complemento utilizando la imagen `velero-plugin-for-vsphere` que personalizó.

   Cuando instale el complemento de Velero para vSphere en un clúster básico, se implementan dos componentes adicionales: una implementación de `backup-driver` y un DaemonSet de `data-manager-for-plugin` en segundo plano. En los clústeres de Tanzu Kubernetes y el clúster supervisor, solo se procede con una implementación de `backup-driver`.

   Cuando se proporciona la imagen de contenedor de `velero-plugin-for-vsphere`, las imágenes de `backup-driver` y `data-manager-for-plugin` coincidentes se analizan mediante un mecanismo de análisis de imágenes.

   Las imágenes de contenedor se formalizan con el siguiente patrón:

   ```
   <Registry endpoint and path>/<Container name>:<Version tag>
   ```

   Cuando se proporciona la imagen de contenedor de `velero-plugin-for-vsphere`, se analizan las imágenes correspondientes de `backup-driver` y `data-manager-for-plugin` con las coincidentes de `<Registry endpoint and path>` y `<Version tag>`.

   Por ejemplo, tenga en cuenta la siguiente imagen de contenedor de `velero-plugin-for-vsphere`:

   ```
   abc.io:8989/x/y/.../z/velero-plugin-for-vsphere:vX.Y.Z
   ```

   Se espera que se extraigan las siguientes imágenes coincidentes de `backup-driver` y `data-manager-for-plugin`:

   ```
   abc.io:8989/x/y/.../z/backup-driver:vX.Y.Z
   abc.io:8989/x/y/.../z/data-manager-for-plugin:vX.Y.Z
   ```

4. Solucione los problemas de la instalación.

Si se produce algún problema o error al analizar las imágenes coincidentes de `backup-driver` y `data-manager-for-plugin`, la instalación recurre a las imágenes correspondientes de los repositorios oficiales de `velerovsphereplugin` en Docker Hub. Los siguientes problemas activan el mecanismo de reserva:

a En la entrada del usuario, se utiliza un nombre de contenedor inesperado en la imagen de `velero-plugin-for-vsphere` personalizada.

   Por ejemplo, se utiliza `x/y/velero-velero-plugin-for-vsphere:v1.1.1`.

b El nombre de la implementación de Velero se personaliza con cualquier otra opción que no sea `velero`. Por ejemplo, se activa un problema si el nombre de la implementación de Velero se actualiza a `velero-server` en el archivo `manifests` de Velero antes de implementar Velero.

   El mecanismo de análisis de imágenes que hay actualmente en `velero-plugin-for-vsphere` solo puede reconocer la implementación de Velero con el nombre fijo, `velero`.

Desinstale el complemento de Velero para vSphere

Siga estos pasos para desinstalar el complemento de Velero para vSphere. Realice los pasos en el orden mencionado.

1 Ejecute la CLI `velero-vsphere` para desinstalar el complemento de Velero para vSphere.

```
./velero-vsphere uninstall -n velero
```

2 Compruebe que se haya eliminado el pod de vSphere denominado `velero`.

```
kubectl get pods -n velero
```

   Si ve que el pod está "Finalizando", espere a que se elimine antes de continuar.

3 Con vSphere Client, elimine el espacio de nombres de vSphere denominado `velero` que creó manualmente.

   Nota No continúe con el siguiente paso hasta que se complete la eliminación del espacio de nombres. Puede utilizar kubectl para comprobar que se eliminó el espacio de nombres `velero` (pero no utilice kubectl para eliminar el espacio de nombres `velero`).

4 Con vSphere Client, desinstale **Velero vSphere Operator** del clúster supervisor.

   a Seleccione el clúster de vCenter en el que está habilitada **Administración de cargas de trabajo**.

   b Seleccione **Configurar > Servicios de vSphere > Descripción general**.

   c Seleccione **Velero vSphere Operator**.

   d Haga clic en **Desinstalar**.

Con esta acción, se desinstala **Velero vSphere Operator** del clúster supervisor. El operador permanece disponible para volverlo a instalar en la página **Administración de cargas de trabajo > Servicios**. Para eliminar el servicio por completo, seleccione **Acciones > Eliminar**.

Realizar copias de seguridad y restaurar pods de vSphere mediante el complemento complemento de Velero para vSphere

Puede utilizar el complemento complemento de Velero para vSphere para crear copias de seguridad y restaurar cargas de trabajo que se ejecutan en pods de vSphere.

Descripción general

Puede utilizar el complemento complemento de Velero para vSphere para realizar copias de seguridad y restaurar cargas de trabajo que se ejecutan en pods de vSphere de clúster supervisor. Puede realizar copias de seguridad y restaurar aplicaciones sin estado y con estado que se ejecutan en pods de vSphere. Para las aplicaciones con estado, utilice el complemento complemento de Velero para vSphere para crear instantáneas de los volúmenes persistentes (Persistent Volumes, VA).

Nota No puede usar Velero independiente con Restic para realizar copias de seguridad y restaurar pods de vSphere. Debe utilizar el complemento complemento de Velero para vSphere instalado en clúster supervisor.

Requisitos previos

Antes de poder realizar una copia de seguridad y restaurar pods de vSphere, debe instalar y configurar el complemento de complemento de Velero para vSphere. Consulte Instalar y configurar el complemento de Velero para vSphere en el clúster supervisor.

Nota El complemento de complemento de Velero para vSphere no realiza una copia de seguridad ni restaura el estado de clúster supervisor.

Realizar una copia de seguridad de pod de vSphere

Para realizar una copia de seguridad de pod de vSphere sin estado, ejecute el siguiente comando:

```
velero backup create <backup name> --include-namespaces=my-namespace
```

La copia de seguridad se marca como `Completed` después de que se hayan tomado todas las instantáneas locales y de que los metadatos de Kubernetes se carguen en el almacén de objetos. Sin embargo, la copia de seguridad de las instantáneas de volumen se produce de forma asíncrona y puede seguir ocurriendo en segundo plano y tardar algún tiempo en completarse.

Puede comprobar el estado de las instantáneas de volumen supervisando instantáneas y cargando recursos personalizados.

CRD de instantánea

Para cada instantánea de volumen, se crea un recurso personalizado de instantánea en el mismo espacio de nombres que la PVC a la que se crea la instantánea. Puede obtener todas las instantáneas en el espacio de nombres de PVC ejecutando el siguiente comando.

```
kubectl get -n <pvc namespace> snapshot
```

La CRD de instantánea tiene varias fases para el campo de `status.phase`, entre ellas, las siguientes:

Estado	Descripción
New	Aún no procesada
Snapshotted	Se tomó una instantánea local
SnapshotFailed	Se produjo un error en la instantánea local
Uploading	Se está cargando la instantánea
Uploaded	Se cargó la instantánea
UploadFailed	No se pudo cargar la instantánea
Canceling	Se está cancelando la carga de la instantánea
Canceled	Se canceló la carga de la instantánea
CleanupAfterUploadFailed	Error en la limpieza de la instantánea local después de la carga de la instantánea

Cargar CRD

Para cada instantánea de volumen que se cargará en el almacén de objetos, se creará un CR de carga en el mismo espacio de nombres que Velero. Puede obtener todas las cargas en el espacio de nombres de Velero ejecutando el siguiente comando.

```
kubectl get -n <velero namespace> upload
```

La carga de CRD tiene varias fases para el campo de `status.phase`, entre las que se incluyen las siguientes:

Estado	Descripción
New	Aún no procesada
InProgress	Carga en curso
UploadError	Error al cargar
CleanupFailed	Error al eliminar la instantánea local después de la carga Se reintentará

Estado	Descripción
Canceling	Se está cancelando la carga Puede producirse si se llama a `velero backup delete` mientras la carga de instantáneas está en curso
Canceled	Carga cancelada

Las cargas de errores de carga se volverán a intentar periódicamente. En ese momento, su fase volverá a En curso. Una vez que una carga se haya completado correctamente, su registro permanecerá durante un período de tiempo y, finalmente, se eliminará.

Restaurar una pod de vSphere

Para restaurar una carga de trabajo de pod de vSphere de la que se realizó una copia de seguridad mediante el complemento complemento de Velero para vSphere, realice los siguientes pasos.

1 Cree un espacio de nombres de vSphere para la carga de trabajo que restaurará.

2 Configure la directiva de almacenamiento para el espacio de nombres.

3 Ejecute el siguiente comando de Velero para restaurar la carga de trabajo:

```
velero restore create --from-backup backup-name
```

La restauración de Velero se marcará como `Completed` cuando las instantáneas de volumen y otros metadatos de Kubernetes se hayan restaurado correctamente en el clúster actual. En este punto, también se completan todas las tareas del complemento de vSphere relacionadas con esta restauración. En el caso de las copias de seguridad de Velero, no hay tareas de movimiento de datos asíncronas por detrás.

Antes de que la restauración de Velero sea `Completed`, puede comprobar el estado de la restauración de volúmenes supervisando CloneFromSnapshots/Descargar CSR como se indica a continuación.

CRD de CloneFromSnapshots

Para la restauración a partir de cada instantánea de volumen, se creará un CR de CloneFromSnapshots en el mismo espacio de nombres que la PVC a la que se creó originalmente una instantánea. Podemos obtener todos los CloneFromSnapshots de PVC ejecutando el siguiente comando.

```
kubectl -n <pvc namespace> get clonefromsnapshot
```

CRD de CloneFromSnapshots tiene varias fases para el campo `status.phase`, entre ellas las siguientes:

Estado	Descripción
New	No se completó la clonación de la instantánea
Completed	Se completó la clonación de la instantánea
Failed	Error en la clonación de instantánea

Descargar CRD

Desde cada restauración de instantánea de volumen que se descargará del almacén de objetos, se creará un CR de descarga en el mismo espacio de nombres que Velero. Podemos obtener todas las descargas en el espacio de nombres de Velero ejecutando el siguiente comando.

```
kubectl -n <velero namespace> get download
```

La CRD de descarga tiene varias fases para el campo `status.phase`, entre las que se incluyen las siguientes:

Estado	Descripción
New	Aún no procesada
InProgress	Descarga en curso
Completed	Se completó la descarga
Retry	Se volverá a intentar la descarga. Cuando se produce un error durante la descarga de los datos de copia de seguridad, se vuelve a intentar la descarga
Failed	Error en la descarga

Instalar y configurar el complemento de Velero para vSphere en un clúster de Tanzu Kubernetes

Puede utilizar el complemento de Velero para vSphere para realizar una copia de seguridad y restauración de las cargas de trabajo que se ejecutan en un clúster de Tanzu Kubernetes mediante la instalación del complemento de Velero para vSphere en ese clúster.

Descripción general

complemento de Velero para vSphere proporciona una solución para realizar copias de seguridad y restauración de las cargas de trabajo del clúster de Tanzu Kubernetes para los clústeres aprovisionados por servicio Tanzu Kubernetes Grid. Para cargas de trabajo persistentes, el complemento de Velero para vSphere le permite tomar instantáneas de los volúmenes persistentes.

Nota Si necesita portabilidad para las cargas de trabajo del clúster de Tanzu Kubernetes de las que desea realizar una copia de seguridad y restauración, no utilice el complemento de Velero para vSphere. Para la portabilidad entre clústeres de Kubernetes, utilice Velero independiente con Restic. Consulte Instalar y configurar Velero y Restic independientes en un clúster de Tanzu Kubernetes.

Requisito previo: Instale el complemento de Velero para vSphere en el clúster supervisor

Para la instalación del complemento de Velero para vSphere en un clúster de Tanzu Kubernetes, se requiere que el clúster supervisor tenga instalado el complemento de Velero para vSphere. Además, el clúster supervisor debe estar configurado con redes de NSX-T.

Antes de instalar el complemento de Velero para vSphere en un clúster de Tanzu Kubernetes, primero debe instalar el complemento de Velero para vSphere en el clúster supervisor. Consulte Instalar y configurar el complemento de Velero para vSphere en el clúster supervisor.

Instalar la CLI de Velero en una estación de trabajo Linux

La CLI de Velero es la herramienta estándar para interactuar con Velero. La CLI de Velero proporciona más funcionalidad que la CLI del complemento de Velero para vSphere (`velero-vsphere`) y es necesaria para realizar copias de seguridad y restauración de las cargas de trabajo del clúster de Tanzu Kubernetes.

Instale la CLI de Velero en una estación de trabajo Linux. Idealmente, este es el mismo host de salto en el que se ejecutan las CLI asociadas para el entorno de vSphere with Tanzu, incluidos `kubectl`, `kubectl-vsphere` y `velero-vsphere`.

Complete los siguientes pasos para instalar la CLI de Velero.

1 Descargue la versión compatible de la CLI de Velero desde la página de descargas de productos de VMware. Para obtener más información sobre las versiones de Velero compatibles, consulte las notas de la versión.

2 Abra una línea de comandos y cambie el directorio a la descarga de la CLI de Velero.

```
gunzip velero-linux-v1.x.x_vmware.1.gz
```

3 Compruebe el archivo binario de Velero.

```
ls -l

-rw-r--r-- 1 root root 7142128 Aug 14 14:14 velero-linux-v1.x.x_vmware.1
```

4 Otorgue permisos de ejecución a la CLI de Velero.

```
chmod +x velero-linux-v1.x.x_vmware.1
```

5 Haga que la CLI de Velero esté disponible globalmente, para ello, muévala a la ruta del sistema.

```
cp velero-linux-v1.x.x_vmware.1 /usr/local/bin/velero
```

6 Compruebe la instalación de la CLI de Velero.

```
velero version

Client:
    Version: v1.x.x
```

Obtener los detalles del depósito compatible con S3

Para mayor comodidad, los pasos asumen que está utilizando el mismo almacén de objetos compatible con S3 que configuró cuando instaló el complemento de Velero para vSphere en el clúster supervisor. En producción, es posible que desee crear un almacén de objetos independiente.

Para instalar el complemento de Velero para vSphere, deberá proporcionar la siguiente información sobre el almacén de objetos compatible con S3.

Elemento de datos	Valor de ejemplo
s3Url	http://my-s3-store.example.com
aws_access_key_id	ACCESS-KEY-ID-STRING
aws_secret_access_key	SECRET-ACCESS-KEY-STRING

Cree un nombre de archivo de secretos `s3-credentials` con la siguiente información. Debe hacer referencia a este archivo cuando instale el complemento de Velero para vSphere.

```
aws_access_key_id = ACCESS-KEY-ID-STRING
aws_secret_access_key = SECRET-ACCESS-KEY-STRING
```

Instalar el complemento de Velero para vSphere en el clúster de Tanzu Kubernetes

Debe utilizar la CLI de Velero para instalar el complemento de Velero para vSphere en el clúster de destino de Tanzu Kubernetes del que desea realizar una copia de seguridad y restauración.

El contexto de la CLI de Velero seguirá automáticamente el contexto de `kubectl`. Antes de ejecutar los comandos de la CLI de Velero para instalar Velero y el complemento de Velero para vSphere en el clúster de destino, asegúrese de establecer el contexto de `kubectl` en el clúster de destino.

1 Utilice complemento de vSphere para kubectl para autenticarse en clúster supervisor. Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

2 Establezca el contexto de `kubectl` en el clúster de destino de Tanzu Kubernetes.

```
kubectl config use-context TARGET-TANZU-KUBERNETES-CLUSTER
```

3 Ejecute el siguiente comando de la CLI de Velero para instalar Velero en el clúster de destino.

Reemplace los valores de marcador de posición de los campos **BUCKET-NAME**, **REGION** (dos instancias) y **s3Url** con los valores adecuados. Si se desvió de cualquiera de las instrucciones anteriores, ajuste también esos valores, como el nombre o la ubicación del archivo de secretos, el nombre del espacio de nombres `velero` creado manualmente, etc.

```
./velero install --provider aws \
--bucket BUCKET-NAME \
--secret-file ./s3-credentials \
--features=EnableVSphereItemActionPlugin \
--plugins velero/velero-plugin-for-aws:v1.1.0 \
--snapshot-location-config region=REGION \
--backup-location-config region=REGION,s3ForcePathStyle="true",s3Url=http://my-s3-
store.example.com
```

4 Instale el complemento de Velero para vSphere en el clúster de destino. El Velero instalado se comunicará con el servidor de API de Kubernetes para instalar el complemento.

```
velero plugin add vsphereveleroplugin/velero-plugin-for-vsphere:1.1.0
```

Desinstalar el complemento de Velero para vSphere del clúster

Siga estos pasos para desinstalar el complemento de Velero para vSphere.

1 Establezca el contexto de `kubectl` en el clúster de destino de Tanzu Kubernetes.

```
kubectl config use-context TARGET-TANZU-KUBERNETES-CLUSTER
```

2 Para desinstalar el complemento, ejecute el siguiente comando para eliminar el InitContainer de velero-plugin-for-vsphere de la implementación de Velero.

```
velero plugin remove vsphereveleroplugin/velero-plugin-for-vsphere:1.1.0
```

3 Para completar la desinstalación, elimine la implementación del controlador de copia de seguridad y los CRD relacionados.

```
kubectl -n velero delete deployment.apps/backup-driver
```

```
kubectl delete crds \
backuprepositories.backupdriver.cnsdp.vmware.com \
backuprepositoryclaims.backupdriver.cnsdp.vmware.com \
clonefromsnapshots.backupdriver.cnsdp.vmware.com \
deletesnapshots.backupdriver.cnsdp.vmware.com \
snapshots.backupdriver.cnsdp.vmware.com
```

```
kubectl delete crds uploads.datamover.cnsdp.vmware.com downloads.datamover.cnsdp.vmware.com
```

Copia de seguridad y restauración de cargas de trabajo del clúster de Tanzu Kubernetes mediante complemento de Velero para vSphere

Puede realizar una copia de seguridad y restaurar las cargas de trabajo del clúster de Tanzu Kubernetes mediante complemento de Velero para vSphere. Sin embargo, si necesita portabilidad, utilice Velero independiente.

Requisitos previos

Para realizar una copia de seguridad y restaurar las cargas de trabajo de los clústeres de Tanzu Kubernetes mediante complemento de Velero para vSphere, primero debe instalar Velero y el complemento complemento de Velero para vSphere en el clúster de destino. Consulte Instalar y configurar el complemento de Velero para vSphere en un clúster de Tanzu Kubernetes.

Copia de seguridad de una carga de trabajo

A continuación se muestra un comando de ejemplo para crear una copia de seguridad de Velero.

```
velero backup create <backup name> --include-namespaces=my-namespace
```

La copia de seguridad de Velero se marcará como `Completed` después de que se hayan tomado todas las instantáneas locales y se hayan cargado los metadatos de Kubernetes, excepto las instantáneas de volumen, en el almacén de objetos. En este punto, las tareas de movimiento de datos asincrónicas, es decir, la carga de instantáneas de volumen, aún se están realizando en segundo plano y pueden tardar algún tiempo en completarse. Podemos comprobar el estado de las instantáneas de volumen mediante la supervisión de los recursos personalizados (CR) de instantánea.

Instantáneas

Las instantáneas se utilizan para realizar copias de seguridad de volúmenes persistentes. Para cada instantánea de volumen, se crea un CR de instantánea en el mismo espacio de nombres que la notificación de volumen persistente (PVC) de que se crea una instantánea.

Puede obtener todas las instantáneas en el espacio de nombres de PVC ejecutando el siguiente comando.

```
kubectl get -n <pvc namespace> snapshot
```

La definición de recursos personalizados (CRD) de instantánea tiene varias fases para el campo `.status.phase`, que incluyen lo siguiente:

Fase de instantánea	Descripción
New	Aún no procesada
Snapshotted	Se tomó una instantánea local
SnapshotFailed	Se produjo un error en la instantánea local
Uploading	Se está cargando la instantánea
Uploaded	Se cargó la instantánea
UploadFailed	No se pudo cargar la instantánea
Canceling	Se está cancelando la carga de la instantánea
Canceled	Se canceló la carga de la instantánea
CleanupAfterUploadFailed	Se produjo un error en la limpieza de la instantánea local después de la carga de la instantánea

Restaurar una carga de trabajo

A continuación se muestra un comando de ejemplo de restauración de Velero.

```
velero restore create --from-backup <velero-backup-name>
```

La restauración de Velero se marcará como `Completed` cuando las instantáneas de volumen y otros metadatos de Kubernetes se hayan restaurado correctamente en el clúster actual. En este punto, también se completan todas las tareas del complemento de vSphere relacionadas con esta restauración. No hay tareas de movimiento de datos asincrónicas en segundo plano como en el caso de la copia de seguridad de Velero.

CloneFromSnapshots

Para restaurar desde cada instantánea de volumen, se creará un recurso personalizado (CR) `CloneFromSnapshot` en el mismo espacio de nombres que la PVC que se creó originalmente. Podemos obtener todos los CloneFromSnapshots de PVC ejecutando el siguiente comando.

```
kubectl -n <pvc namespace> get clonefromsnapshot
```

CloneFromSnapshot CRD tiene algunas fases clave para el campo `.status.phase`:

Fase de instantánea	Descripción
New	No se completó la clonación de la instantánea
InProgress	La instantánea del volumen de vSphere se está descargando desde el repositorio remoto
Completed	Se completó la clonación de la instantánea
Failed	Error en la clonación de la instantánea

Instalar y configurar Velero y Restic independientes en un clúster de Tanzu Kubernetes

Para realizar copias de seguridad y restauración de cargas de trabajo en Tanzu Kubernetes, cree un almacén de datos e instale Velero con Restic en el clúster de Kubernetes.

Descripción general

Los clústeres de Tanzu Kubernetes se ejecutan en nodos de máquina virtual. Para realizar una copia de seguridad y restauración de clústeres de Tanzu Kubernetes, instale Velero y Restic en el clúster.

Requisitos previos

Asegúrese de que el entorno cumpla con los siguientes requisitos previos para instalar Velero y Restic a fin de realizar copias de seguridad y restauración de cargas de trabajo que se ejecutan en clústeres de Tanzu Kubernetes.

- Una máquina virtual Linux con suficiente almacenamiento para almacenar varias copias de seguridad de cargas de trabajo. Debe instalar MinIO en esta máquina virtual.
- Una máquina virtual Linux en la que están instaladas Herramientas de la CLI de Kubernetes para vSphere, lo que incluye complemento de vSphere para kubectl y kubectl. Debe instalar la CLI de Velero en esta máquina virtual cliente. Si no tiene una máquina virtual de este tipo, puede instalar la CLI de Velero de forma local, pero debe ajustar los pasos de instalación según corresponda.
- El entorno de Kubernetes tiene acceso a Internet y la máquina virtual cliente puede acceder a él.

Instalar y configurar el almacén de objetos minIO

Velero requiere un almacén de objetos compatible con S3 como el destino de las copias de seguridad de la cargas de trabajo de Kubernetes. Velero admite varios proveedores de almacenes de objetos de este tipo. Por simplicidad, estas instrucciones utilizan MinIO, un servicio de almacenamiento compatible con S3 que se ejecuta localmente en la máquina virtual del almacén de objetos.

1 Instale MinIO.

```
wget https://dl.min.io/server/minio/release/linux-amd64/minio
```

2 Otorgue permisos de ejecución a MinIO.

```
chmod +x minio
```

3 Cree un directorio en el sistema de archivos para MinIO.

```
mkdir /DATA-MINIO
```

4 Inicie el servidor MinIO.

```
./minio server /DATA-MINIO
```

5 Una vez iniciado el servidor MinIO, se le proporcionarán detalles importantes de la instancia del almacén de datos, incluidos la URL del endpoint, AccessKey y SecretKey. Registre la URL de endpoint, AccessKey y SecretKey en la tabla.

Metadatos del almacén de datos	Valor
URL de endpoint	
AccessKey	
SecretKey	

6 Abra un navegador a la URL del endpoint del servidor MinIO y desplácese hasta el almacén de datos de MinIO.

7 Inicie sesión en el servidor MinIO y proporcione AccessKey y SecretKey.

8 Para habilitar MinIO como servicio, descargue el script `minio.service` para configurar MinIO para inicio automático.

```
curl -O https://raw.githubusercontent.com/minio/minio-service/master/linux-systemd/
minio.service
```

9 Edite el script `minio.service` y agregue el siguiente valor para `ExecStart`.

```
ExecStart=/usr/local/bin/minio server /DATA-MINIO path
```

10 Guarde el script revisado.

11 Configure el servicio MinIO mediante la ejecución de los siguientes comandos.

```
cp minio.service /etc/systemd/system
cp minio /usr/local/bin/
systemctl daemon-reload
systemctl start minio
systemctl status minio
systemctl enable minio
```

12 Cree un depósito MinIO para realizar una copia de seguridad y restauración; para ello, inicie el explorador MinIO e inicie sesión en el almacén de objetos.

13 Haga clic en el icono Crear depósito.

14 Introduzca el nombre del depósito, por ejemplo: `my-cluster-backups`.

15 Compruebe que se haya creado el depósito.

16 De forma predeterminada, un nuevo depósito MinIO es de solo lectura. Para una copia de seguridad y restauración independientes de Velero, el depósito MinIO debe ser de lectura y escritura. Para establecer el depósito en lectura y escritura, selecciónelo y haga clic en el vínculo de puntos suspensivos (puntos).

17 Seleccione **Editar directiva**.

18 Cambie la directiva a **Lectura y escritura**.

19 Haga clic en **Agregar**.

20 Para cerrar el cuadro de diálogo, haga clic en la X.

Instalar la CLI de Velero

Instale la CLI de Velero en el cliente de máquina virtual o en la máquina local.

1 Descargue la versión compatible del archivo binario de Velero firmado para vSphere with Tanzu de la página de descargas de productos VMware.

Nota Debe utilizar el archivo binario de Velero firmado por VMware para poder recibir soporte de VMware.

2 Abra una línea de comandos y cambie el directorio a la descarga de la CLI de Velero.

3 Descomprima el archivo de descarga. Por ejemplo:

```
gunzip velero-linux-vX.X.X_vmware.1.gz
```

4 Compruebe el archivo binario de Velero.

```
ls -l
```

5 Otorgue permisos de ejecución a la CLI de Velero.

```
chmod +x velero-linux-vX.X.X_vmware.1
```

6 Haga que la CLI de Velero esté disponible globalmente, para ello, muévala a la ruta del sistema:

```
cp velero-linux-vX.X.X_vmware.1 /usr/local/bin/velero
```

7 Compruebe la instalación.

```
velero version
```

Instalar Velero y Restic en el clúster de Tanzu Kubernetes

El contexto de la CLI de Velero seguirá automáticamente el contexto de kubectl. Antes de ejecutar los comandos de la CLI de Velero para instalar Velero y Restic en el clúster de destino, establezca el contexto de kubectl.

1 Recupere el nombre del depósito MinIO. Por ejemplo, `my-cluster-backups`.

2 Obtenga AccessKey y SecretKey para el depósito MinIO.

3 Establezca el contexto del clúster de Kubernetes de destino para que la CLI de Velero sepa en qué clúster trabajar.

```
kubectl config use-context tkgs-cluster-name
```

4 Cree un archivo de secretos denominado `credentials-minio`. Actualice el archivo con las credenciales de acceso al servidor MinIO que recopiló. Por ejemplo:

```
aws_access_key_id = 0XXNO8JCCGV41QZBV0RQ
aws_secret_access_key = clZ1bf8Ljkvkmq7fHucrKCkxV39BRbcycGeXQDfx
```

Nota Si recibe el mensaje de error "Error al obtener un almacén de copias de seguridad" con la descripción "NoCredentialProviders: no hay proveedores válidos en la cadena", anteponga la línea `[default]` al principio del archivo de credenciales. Por ejemplo:

```
[default]
aws_access_key_id = 0XXNO8JCCGV41QZBV0RQ
aws_secret_access_key = clZ1bf8Ljkvkmq7fHucrKCkxV39BRbcycGeXQDfx
```

5 Guarde el archivo y compruebe que esté en su lugar.

```
ls
```

6 Ejecute el siguiente comando para instalar Velero y Restic en el clúster de Kubernetes de destino. Reemplace ambas URL por la URL de la instancia de MinIO.

```
velero install \
--provider aws \
--plugins velero/velero-plugin-for-aws:v1.0.0 \
--bucket tkgs-velero \
--secret-file ./credentials-minio \
--use-volume-snapshots=false \
--use-restic \
--backup-location-config \
region=minio,s3ForcePathStyle="true",s3Url=http://10.199.17.63:9000,publicUrl=http://
10.199.17.63:9000
```

7 Compruebe la instalación de Velero y Restic.

```
kubectl logs deployment/velero -n velero
```

8 Compruebe el espacio de nombres `velero`.

```
kubectl get ns
```

9 Compruebe los pods `velero` y `restic`.

```
kubectl get all -n velero
```

Solucionar problemas de DaemonSet de Restic (si es necesario)

Para ejecutar el DaemonSet de Restic de tres pods en un clúster de Kubernetes, es posible que deba actualizar la especificación de DaemonSet de Restic y modificar el hostPath. Para obtener más información sobre este problema, consulte Integración de Restic en la documentación de Velero.

1 Compruebe el DaemonSet de Restic de tres pods.

```
kubectl get pod -n velero
```

Si los pods tienen el estado CrashLoopBackOff, edítelos de la siguiente manera.

2 Ejecute el comando `edit`.

```
kubectl edit daemonset restic -n velero
```

3 Cambie hostPath de `/var/lib/kubelet/pods` a `/var/vcap/data/kubelet/pods`.

```

- hostPath:
    path: /var/vcap/data/kubelet/pods
```

4 Guarde el archivo.

5 Compruebe el DaemonSet de Restic de tres pods.

```
kubectl get pod -n velero
```

```
NAME                       READY   STATUS    RESTARTS   AGE
restic-5jln8               1/1     Running   0          73s
restic-bpvtq               1/1     Running   0          73s
restic-vg8j7               1/1     Running   0          73s
velero-72c84322d9-le7bd    1/1     Running   0          10m
```

Ajustar los límites de memoria de Velero (si es necesario)

Si la copia de seguridad de Velero devuelve `status=InProgress` durante muchas horas, aumente la configuración de memoria para límites y solicitudes.

1 Ejecute el siguiente comando.

```
kubectl edit deployment/velero -n velero
```

2 Cambie la configuración de memoria para límites y solicitudes desde el valor predeterminado de `256Mi` y `128Mi` a `512Mi` y `256Mi`.

```
ports:
- containerPort: 8085
  name: metrics
  protocol: TCP
resources:
  limits:
    cpu: "1"
    memory: 512Mi
  requests:
    cpu: 500m
    memory: 256Mi
terminationMessagePath: /dev/termination-log
terminationMessagePolicy: File
```

Copia de seguridad y restauración de cargas de trabajo de clúster de Tanzu Kubernetes mediante Restic y Velero independientes

Puede realizar copias de seguridad y restaurar cargas de trabajo de clúster de Tanzu Kubernetes mediante Restic y Velero independientes. Este método es una alternativa al uso de un complemento complemento de Velero para vSphere. La razón principal para usar Velero independiente en lugar del complemento complemento de Velero para vSphere es si se requiere portabilidad. Se requiere Restic para las cargas de trabajo con estado.

Requisitos previos

Para realizar copias de seguridad y restaurar cargas de trabajo de clúster de Tanzu Kubernetes mediante Restic y Velero independientes, debe instalar la versión independiente de estos en el clúster de destino. Consulte Instalar y configurar Velero y Restic independientes en un clúster de Tanzu Kubernetes.

Nota La copia de seguridad y la restauración de un clúster de Kubernetes mediante Velero independiente con Restic le ofrece portabilidad. Esto significa que si desea poder restaurar las cargas de trabajo del clúster en un clúster de Kubernetes no aprovisionado por servicio Tanzu Kubernetes Grid, debe utilizar Velero independiente.

Realizar una copia de seguridad de una aplicación sin estado que se ejecuta en un clúster de Tanzu Kubernetes

La copia de seguridad de una aplicación sin estado que se ejecuta en un clúster de Tanzu Kubernetes requiere el uso de Velero.

En este ejemplo se muestra cómo realizar una copia de seguridad y restaurar una aplicación sin estado de ejemplo mediante la etiqueta `--include namespaces` en la que todos los componentes de la aplicación se encuentran en ese espacio de nombres.

```
velero backup create example-backup --include-namespaces example-backup
```

Debería ver el siguiente mensaje:

```
Backup request "example-backup" submitted successfully.
Run `velero backup describe example-backup` or `velero backup logs example-backup` for more
details.
```

Compruebe la copia de seguridad que se creó.

```
velero backup get
```

```
velero backup describe example-backup
```

Compruebe el depósito Velero en el almacén de objetos compatible con S3, como el servidor MinIO.

Velero escribe algunos metadatos en definiciones de recursos personalizados (Custom Resource Definitions, CRD) de Kubernetes.

```
kubectl get crd
```

Las CRD de Velero permiten ejecutar ciertos comandos, como los siguientes:

```
kubectl get backups.velero.io -n velero
```

```
kubectl describe backups.velero.io guestbook-backup -n velero
```

Restaurar una aplicación sin estado en ejecución en un clúster de Tanzu Kubernetes

La restauración de una aplicación sin estado que se ejecuta en un clúster de Tanzu Kubernetes requiere el uso de Velero.

Para probar la restauración de una aplicación de ejemplo, elimínela.

Elimine el espacio de nombres:

```
kubectl delete ns guestbook
namespace "guestbook" deleted
```

Restaure la aplicación:

```
velero restore create --from-backup example-backup
```

Debería ver el siguiente mensaje:

```
Restore request "example-backup-20200721145620" submitted successfully.
Run `velero restore describe example-backup-20200721145620` or `velero restore logs example-
backup-20200721145620` for more details.
```

Compruebe que la aplicación se restauró:

```
velero restore describe example-backup-20200721145620
```

Ejecute los siguientes comandos para comprobar:

```
velero restore get
```

```
kubectl get ns
```

```
kubectl get pod -n example
```

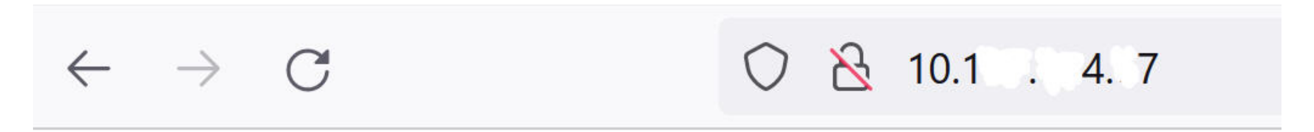
```
kubectl get svc -n example
```

Realizar una copia de seguridad de una aplicación con estado que se ejecuta en un clúster de Tanzu Kubernetes

Realizar una copia de seguridad de una aplicación con estado que se ejecuta en un clúster de Tanzu Kubernetes implica realizar una copia de seguridad de los metadatos de la aplicación y los datos de la aplicación almacenados en un volumen persistente. Para ello, necesita Velero y Restic.

En este ejemplo, utilizaremos la aplicación del libro de visitas. Si se supone que implementó la aplicación del libro de visitas en un clúster de Tanzu Kubernetes. Consulte Tutorial del libro de visitas de Tanzu Kubernetes para obtener instrucciones.

Para que podamos demostrar una copia de seguridad y una restauración con estado, envíe un mensaje a la aplicación del libro de visitas mediante la página web de front-end para que los mensajes persistan. Por ejemplo:





En este ejemplo se muestra cómo realizar una copia de seguridad y restaurar la aplicación del libro de visitas mediante la etiqueta `--include namespace`, así como las anotaciones del pod.

Nota En este ejemplo, se utilizan anotaciones. Sin embargo, ya no se necesitan anotaciones para Velero 1.5 y versiones posteriores. Para no utilizar anotaciones, puede usar la opción `--default-volumes-to-restic` al crear la copia de seguridad. Esto hará una copia de seguridad automática de todos los VA mediante Restic. Consulte https://velero.io/docs/v1.5/restic/ para obtener más información.

Para comenzar el procedimiento de copia de seguridad, obtenga los nombres de los pods:

```
kubectl get pod -n guestbook
```

Por ejemplo:

```
kubectl get pod -n guestbook

NAME                                            READY   STATUS    RESTARTS   AGE
guestbook-frontend-deployment-85595f5bf9-h8cff  1/1     Running          0          55m
guestbook-frontend-deployment-85595f5bf9-lw6tg  1/1     Running          0          55m
guestbook-frontend-deployment-85595f5bf9-wpqc8  1/1     Running          0          55m
redis-leader-deployment-64fb8775bf-kbs6s        1/1     Running          0          55m
redis-follower-deployment-84cd76b975-jrn8v      1/1     Running          0          55m
redis-follower-deployment-69df9b5688-zml4f      1/1     Running          0          55m
```

Los volúmenes persistentes se asocian a los pods de Redis. Debido a que estamos realizando una copia de seguridad de estos pods con estado con Restic, es necesario agregar anotaciones a los pods con estado con el nombre `volumeMount`.

Debe conocer `volumeMount` para anotar el pod con estado. Para obtener `mountName`, ejecute el siguiente comando.

```
kubectl describe pod redis-leader-deployment-64fb8775bf-kbs6s -n guestbook
```

En los resultados, verá `Containers.leader.Mounts: /data` de `redis-leader-data`. Este último token es el nombre `volumeMount` que se utilizará para la anotación del pod principal. Para el seguidor, será `redis-follower-data`. También puede obtener el nombre de `volumeMount` del YAML de origen.

Anote cada uno de los pods de Redis, por ejemplo:

```
kubectl -n guestbook annotate pod redis-leader-64fb8775bf-kbs6s backup.velero.io/backup-
volumes=redis-leader-data
```

Debería ver el siguiente mensaje:

```
pod/redis-leader-64fb8775bf-kbs6s annotated
```

Verifique las anotaciones:

```
kubectl -n guestbook describe pod redis-leader-64fb8775bf-kbs6s | grep Annotations
Annotations:  backup.velero.io/backup-volumes: redis-leader-data
```

```
kubectl -n guestbook describe pod redis-follower-779b6d8f79-5dphr | grep Annotations
Annotations:  backup.velero.io/backup-volumes: redis-follower-data
```

Realice la copia de seguridad de Velero:

```
velero backup create guestbook-backup --include-namespaces guestbook
```

Debería ver el siguiente mensaje:

```
Backup request "guestbook-backup" submitted successfully.
Run `velero backup describe guestbook-pv-backup` or `velero backup logs guestbook-pv-backup`
for more details.
```

Compruebe la copia de seguridad que se creó.

```
velero backup get

NAME                  STATUS      ERRORS   WARNINGS   CREATED
EXPIRES   STORAGE LOCATION   SELECTOR
guestbook-backup      Completed   0        0          2020-07-23 16:13:46 -0700 PDT
29d       default            <none>
```

Compruebe los detalles de la copia de seguridad.

```
velero backup describe guestbook-backup --details
```

Tenga en cuenta que Velero permite ejecutar otros comandos, como:

```
kubectl get backups.velero.io -n velero

NAME               AGE
guestbook-backup   4m58s
```

Y:

```
kubectl describe backups.velero.io guestbook-backup -n velero
```

Restaurar una aplicación con estado en ejecución en un clúster de Tanzu Kubernetes

La restauración de una aplicación con estado que se ejecuta en un clúster de Tanzu Kubernetes implica restaurar tanto los metadatos de la aplicación como los datos de la aplicación almacenados en un volumen persistente. Para ello, necesita Velero y Restic.

En este ejemplo, se supone que se realizó una copia de seguridad de la aplicación de libro de visitas con estado, como se describe en la sección anterior.

Para probar la restauración de la aplicación con estado, elimine su espacio de nombres:

```
kubectl delete ns guestbook
namespace "guestbook" deleted
```

Verifique la eliminación de la aplicación:

```
kubectl get ns
kubectl get pvc,pv --all-namespaces
```

Restaure la aplicación:

```
Restore request "guestbook-backup-20200723161841" submitted successfully.
Run `velero restore describe guestbook-backup-20200723161841` or `velero restore logs
guestbook-backup-20200723161841` for more details.
```

Compruebe que se restauró la aplicación del libro de visitas con estado:

```
velero restore describe guestbook-backup-20200723161841

Name:         guestbook-backup-20200723161841
Namespace:    velero
Labels:       <none>
Annotations:  <none>

Phase:  Completed

Backup:  guestbook-backup

Namespaces:
  Included:  all namespaces found in the backup
  Excluded:  <none>

Resources:
  Included:        *
  Excluded:        nodes, events, events.events.k8s.io, backups.velero.io,
restores.velero.io, resticrepositories.velero.io
  Cluster-scoped:  auto

Namespace mappings:  <none>

Label selector:  <none>

Restore PVs:  auto

Restic Restores (specify --details for more information):
  Completed:  3
```

Ejecute el siguiente comando adicional para verificar la restauración:

```
velero restore get

NAME                                BACKUP               STATUS      ERRORS   WARNINGS
CREATED                         SELECTOR
guestbook-backup-20200723161841     guestbook-backup     Completed   0        0
2021-08-11 16:18:41 -0700 PDT   <none>
```

Compruebe que se restauró el espacio de nombres:

```
kubectl get ns

NAME              STATUS   AGE
default           Active   16d
guestbook         Active   76s
...
velero            Active   2d2h
```

Compruebe que la aplicación se restauró:

```
vkubectl get all -n guestbook

NAME                                 READY   STATUS    RESTARTS   AGE
pod/frontend-6cb7f8bd65-h2pnb        1/1     Running   0          6m27s
pod/frontend-6cb7f8bd65-kwlpr        1/1     Running   0          6m27s
pod/frontend-6cb7f8bd65-snwl4        1/1     Running   0          6m27s
pod/redis-leader-64fb8775bf-kbs6s    1/1     Running   0          6m28s
pod/redis-follower-779b6d8f79-5dphr 1/1     Running   0          6m28s
pod/redis-follower-899c7e2z65-8apnk 1/1     Running   0          6m28s

NAME                                  TYPE           CLUSTER-IP       EXTERNAL-IP
PORT(S)        AGE
service/guestbook-frontend            LoadBalancer   10.10.89.59      10.19.15.99
80:31513/TCP   65s
service/redis-follower                ClusterIP      10.111.163.189   <none>
6379/TCP       65s
service/redis-leader                  ClusterIP      10.111.70.189    <none>
6379/TCP       65s

NAME                                            READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/guestbook-frontend-deployment   3/3     3            3           65s
deployment.apps/redis-follower-deployment       1/2     2            1           65s
deployment.apps/redis-leader-deployment         1/1     1            1           65s

NAME                                                       DESIRED   CURRENT   READY   AGE
replicaset.apps/guestbook-frontend-deployment-56fc5b6b47   3         3         3       65s
replicaset.apps/redis-follower-deployment-6fc9cf5759       2         2         1       65s
replicaset.apps/redis-leader-deployment-7d89bbdbcf         1         1         1       65s
```

Compruebe que se restauren los volúmenes persistentes:

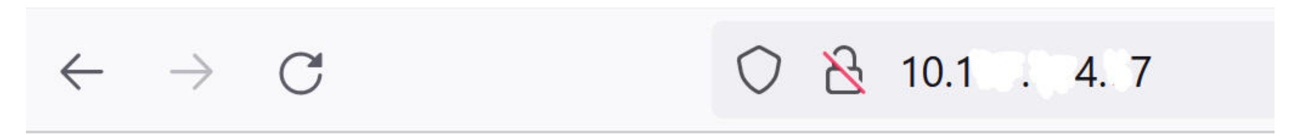
```
kubectl get pvc,pv -n guestbook

NAME                                          STATUS
VOLUME                                        CAPACITY   ACCESS MODES   STORAGECLASS   AGE
persistentvolumeclaim/redis-leader-claim   Bound    pvc-a2f6e6d4-42db-4fb8-
a198-5379a2552509   2Gi        RWO            thin-disk      2m40s
persistentvolumeclaim/redis-follower-claim Bound    pvc-55591938-921f-452a-
b418-2cc680c0560b   2Gi        RWO            thin-disk      2m40s

NAME                                                            CAPACITY   ACCESS MODES   RECLAIM
```

```
POLICY    STATUS    CLAIM                                            STORAGECLASS    REASON    AGE
persistentvolume/pvc-55591938-921f-452a-b418-2cc680c0560b    2Gi        RWO
Delete            Bound     guestbook/redis-follower-claim     thin-disk                    2m40s
persistentvolume/pvc-a2f6e6d4-42db-4fb8-a198-5379a2552509    2Gi        RWO
Delete            Bound     guestbook/redis-leader-claim       thin-disk                    2m40s
```

Por último, acceda al front-end del libro de visitas mediante la dirección IP externa del servicio de front-end del libro de visitas y compruebe que se restauren los mensajes que envió al principio del tutorial. Por ejemplo:



Guestbook

Messages



message 1
message 2
message 3

Copia de seguridad y restauración de vCenter Server

En este tema se describe cómo realizar una copia de seguridad y restaurar la instancia de vCenter Server en el contexto de una implementación de vSphere with Tanzu.

HA del clúster de vCenter

Para admitir un clúster supervisor de alta disponibilidad, vSphere with Tanzu requiere que el clúster de vCenter en el que está habilitado vSphere with Tanzu esté configurado con alta disponibilidad. Para obtener más información, consulte Disponibilidad de vSphere en la documentación de VMware vSphere.

Copia de seguridad y recuperación de vCenter Server

vCenter Server admite la copia de seguridad de archivos en el almacenamiento conectado a la red. Para realizar una copia de seguridad y restauración de vCenter Server, cree una copia de seguridad de vCenter Server principal. Para obtener más información, consulte Copia de seguridad y restauración basadas en archivos de vCenter Server en la documentación de vCenter.

Copia de seguridad y restauración de NSX-T Data Center

Para admitir la funcionalidad de red en el caso de una interrupción de la carga de trabajo de vSphere with Tanzu, realice una copia de seguridad y restaure NSX-T Data Center.

Requisitos

Para realizar una copia de seguridad y restaurar NSX-T Data Center, se supone que se implementaron 3 nodos de NSX Manager y que hay una VIP de HA configurada para acceder al plano de administración de NSX. Además, hay al menos 2 nodos de Edge implementados con una VIP de HA para los nodos de Edge. Para obtener más información, consulte Configurar NSX-T Data Center para vSphere with Tanzu.

Copia de seguridad y restauración de NSX-T

NSX-T Data Center proporciona una copia de seguridad y recuperación en el producto que admite la copia de seguridad y la restauración de los nodos y los objetos de NSX Manager. Para obtener más información, consulte Copia de seguridad y restauración de NSX Manager en la documentación de NSX-T.

Solucionar problemas en vSphere with Tanzu

19

Siga las prácticas recomendadas y las técnicas de solución de problemas siguientes para su infraestructura en vSphere with Tanzu.

Este capítulo incluye los siguientes temas:

- Prácticas recomendadas y solución de problemas de almacenamiento
- Solucionar problemas de redes
- Solucionar problemas de NSX Advanced Load Balancer
- Solucionar problemas de actualización de la topología de red
- Solucionar problemas de clústeres de Tanzu Kubernetes
- Solución de problemas de administración de cargas de trabajo

Prácticas recomendadas y solución de problemas de almacenamiento

Utilice las siguientes prácticas recomendadas y técnicas de solución de problemas en su entorno de almacenamiento de vSphere with Tanzu.

Usar reglas antiafinidad para máquinas virtuales del plano de control en almacenes de datos que no sean de vSAN

Cuando use almacenes de datos que no sean de vSAN en el clúster con vSphere with Tanzu, coloque las tres máquinas virtuales del plano de control en distintos almacenes de datos por motivos de disponibilidad.

Debido a que las máquinas virtuales del plano de control son administradas por el sistema, no se las puede migrar manualmente. Utilice una combinación de un clúster de almacenes de datos y Storage DRS para volver a equilibrar las máquinas virtuales del plano de control y colocarlas en almacenes de datos independientes.

Procedimiento

1 En vSphere Client, cree un clúster de almacenes de datos.

   a Vaya a los centros de datos.

   b Haga clic con el botón secundario en el objeto del centro de datos y seleccione **Nuevo clúster de almacenes de datos**.

   c Asigne un nombre al clúster de almacenes de datos y asegúrese de que **Activar Storage DRS** esté habilitado.

   d Establezca el nivel de automatización del clúster en **Sin automatización (modo manual)**.

   e Deje la configuración predeterminada del tiempo de ejecución de Storage DRS.

   f Seleccione el clúster de ESXi habilitado con vSphere with Tanzu.

   g Seleccione todos los almacenes de datos compartidos para agregar al clúster de almacenes de datos.

   h Haga clic en **Finalizar**.

2 Defina las reglas de Storage DRS para las máquinas virtuales del plano de control.

   a Desplácese hasta el clúster de almacenes de datos.

   b Haga clic en la pestaña **Configurar** y en **Reglas**, en **Configuración**.

   c Haga clic en el icono **Agregar** e introduzca el nombre para la regla.

   d Asegúrese de que **Habilitar regla** esté activado.

   e Establezca **Tipo de regla** en **Antiafinidad de máquina virtual**.

   f Haga clic en el icono **Agregar** y seleccione las tres máquinas virtuales del plano de control de supervisor.

   g Haga clic en **Aceptar** para finalizar la configuración.

3 Cree reemplazos de máquinas virtuales.

   a Desplácese hasta el clúster de almacenes de datos.

   b Haga clic en la pestaña **Configurar** y en **Reemplazos de máquinas virtuales**, en **Configuración**.

   c Haga clic en el icono **Agregar** y seleccione las tres máquinas virtuales del plano de control.

   d Para habilitar el nivel de automatización de Storage DRS, active la casilla de verificación **Reemplazar** y establezca el valor en **Totalmente automatizado**.

   e Haga clic en **Finalizar**.

Resultados

Esta tarea solo habilita Storage DRS para las máquinas virtuales del plano de control y vuelve a equilibrar las máquinas virtuales para que se encuentren en almacenes de datos diferentes.

Una vez que se llevan a cabo las operaciones de Storage vMotion, puede eliminar las reglas y los reemplazos de SDRS, deshabilitar Storage DRS y eliminar el clúster de almacenes de datos.

La directiva de almacenamiento eliminada de vSphere sigue apareciendo como clase de almacenamiento Kubernetes

Cuando se utiliza vSphere Client para eliminar la directiva de almacenamiento de vCenter Server o un espacio de nombres en el clúster supervisor, la clase de almacenamiento coincidente permanece en el entorno de Kubernetes, pero no se puede utilizar.

Problema

Si ejecuta el comando **`kubectl get sc`**, el resultado seguirá mostrando la clase de almacenamiento como disponible en el espacio de nombres. Sin embargo, esta no se podrá usar. Por ejemplo, se produce un error al intentar usar la clase de almacenamiento para una nueva notificación de volumen persistente.

Si una implementación de Kubernetes ya utiliza la clase de almacenamiento, es posible que la implementación se comporte de forma impredecible.

Solución

1 Para comprobar qué clases de almacenamiento hay en el espacio de nombres, ejecute el comando **`kubectl describe namespace`** ***`namespace_name`***.

   La salida de este comando no muestra la clase de almacenamiento si se elimina la directiva de almacenamiento coincidente.

2 Si una implementación ya utiliza la clase de almacenamiento, restaure la clase de almacenamiento.

   a Utilice vSphere Client para crear una nueva directiva de almacenamiento con el mismo nombre que la directiva que eliminó.

      Por ejemplo, si eliminó la directiva *Oro*, asigne el nombre *Oro* a la nueva directiva. Consulte Crear directivas de almacenamiento para vSphere with Tanzu.

   b Asigne la directiva al espacio de nombres.

      Consulte Cambiar la configuración de almacenamiento en un espacio de nombres.

      Después de asignar la directiva al espacio de nombres, vSphere with Tanzu elimina la clase de almacenamiento anterior y crea una clase de almacenamiento coincidente con el mismo nombre.

Usar almacenamiento externo con vSAN Direct

Al utilizar vSAN Direct en el entorno vSphere with Tanzu, se puede usar un almacenamiento compartido externo para almacenar máquinas virtuales internas de administración y otros metadatos.

Problema

Al implementar un clúster de vSAN Direct homogéneo, debe crear un almacén de datos de vSAN replicado en cada host ESXi del clúster para almacenar máquinas virtuales de administración de vSphere with Tanzu y otros metadatos. El almacén de datos de vSAN consume espacio, requiere un controlador de E/S adicional en cada host y limita la configuración de hardware en la que vSAN Direct puede ser compatible.

En lugar de configurar el almacén de datos de vSAN, puede usar el almacenamiento compartido externo para almacenar las máquinas virtuales internas de administración y otros metadatos.

Solución

1 Si vSAN o vSAN Direct se implementaron en hosts ESXi del clúster, borre los hosts de cualquier configuración.

   a Elimine los discos asignados a vSAN o vSAN Direct. Consulte Quitar grupos de discos o dispositivos de vSAN.

   b (opcional) Utilice el script a fin de etiquetar discos en los hosts para vSAN Direct. Consulte Utilizar un script para etiquetar dispositivos de almacenamiento para vSAN Direct.

2 Utilice VMware Cloud Foundation para crear un dominio de carga de trabajo con almacenamiento externo.

   Asegúrese de seleccionar una de las opciones de almacenamiento, como NFS, vVols o FC. Solo se puede seleccionar una de estas opciones.

   Para obtener más información, consulte *Trabajo con dominios de carga de trabajo* en la Guía de operaciones y administración de VMware Cloud Foundation.

   Este paso implementa un dominio de carga de trabajo con vCenter Server y los hosts ESXi especificados. El almacenamiento externo se monta en todos los hosts y se agrega al clúster predeterminado.

3 Habilite vSAN.

   Asegúrese de que no haya discos reclamados para vSAN.

   Para obtener más información, consulte Habilitar vSAN en un clúster existente.

   Este paso crea un almacén de datos de vSAN de cero bytes con la red de vSAN. No se usan discos locales para vSAN.

4 Reclame los discos locales en los hosts para vSAN Direct.

   Para obtener información, consulte Configurar vSAN Direct para vSphere with Tanzu.

   Por cada dispositivo que reclame, vSAN Direct creará un almacén de datos independiente.

5 Cree directivas de almacenamiento para vSAN Direct.

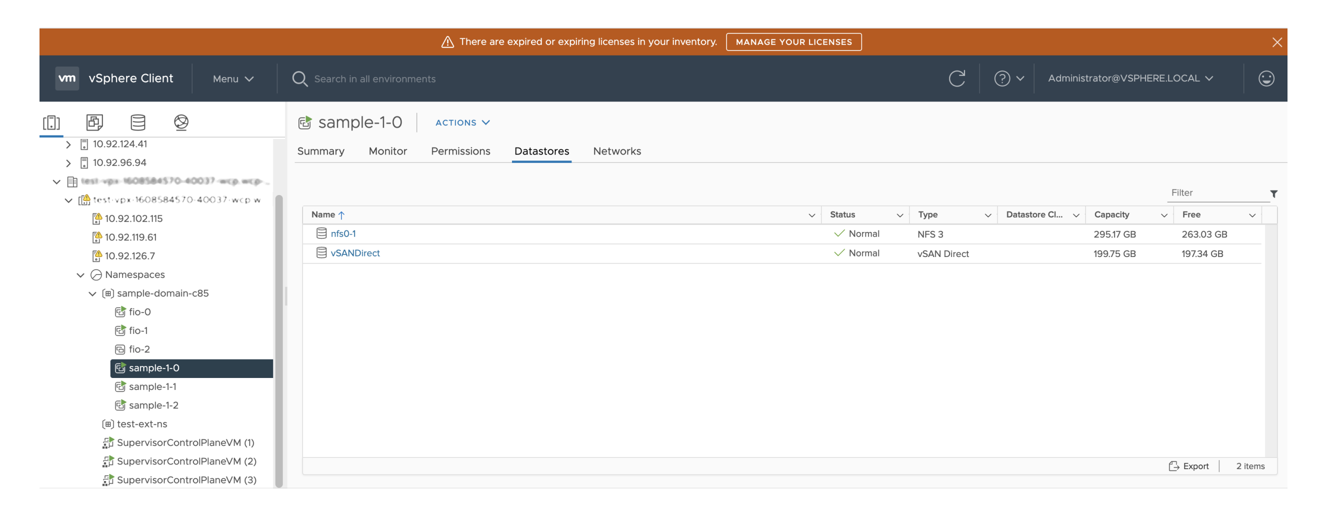
   Para obtener información, consulte Crear directiva de almacenamiento de vSAN Direct.

6 Configure y habilite la administración de cargas de trabajo.

   Para obtener información, consulte Capítulo 5 Configurar y administrar un clúster supervisor.

Ejemplo

En este ejemplo, una configuración incluye almacenamiento NFS externo y un almacén de datos de vSAN Direct. Las máquinas virtuales de plano de control de pods de vSphere se ejecutan en el almacenamiento NFS externo. Las notificaciones de volumen persistente se ejecutan en vSAN Direct.



Solucionar problemas de redes

Puede solucionar los problemas de redes que se podrían encontrar al configurar vSphere with Tanzu con NSX.

Registrar vCenter Server en NSX Manager

En determinadas circunstancias, es posible que deba volver a registrar la instancia de OIDC de vCenter Server en NSX Manager (por ejemplo, cuando el FQDN o el PNID de vCenter Server cambian).

Procedimiento

1 Conéctese al dispositivo vCenter Server mediante SSH.

2 Ejecute el comando `shell`.

3 Para obtener la huella digital de vCenter Server, ejecute el comando – `openssl s_client -connect <vcenterserver-FQDN:443 </dev/null 2>/dev/null | openssl x509 -fingerprint -sha256 -noout -in /dev/stdin`.

   Se mostrará la huella digital. Por ejemplo, `08:77:43:29:E4:D1:6F:29:96:78:5F:BF:D6:45:21:F4:0E:3B:2A:68:05:99:C3:A4:89:8F:F2:0B:EA:3A:BE:9D`

4 Copie la huella digital SHA256 y elimine los dos puntos.

```
08774329E4D16F2996785FBFD64521F40E3B2A680599C3A4898FF20BEA3ABE9D
```

5 Para actualizar la instancia de OIDC de vCenter Server, ejecute el siguiente comando:

```
curl --location --request POST 'https://<NSX-T_ADDRESS>/api/v1/trust-management/oidc-uris'
\
    --header 'Content-Type: application/json' \
    --header 'Authorization: Basic <AUTH_CODE>' \
    --data-raw '{
 "oidc_type": "vcenter",
     "oidc_uri": "https://<VC_ADDRESS>/openidconnect/vsphere.local/.well-known/openid-
configuration",
     "thumbprint": "<VC_THUMBPRINT>"
    }'
```

No se puede cambiar la contraseña de NSX Appliance

Es posible que no pueda cambiar la contraseña de NSX Appliance para los usuarios `root`, `admin` o `audit`.

Problema

Puede que se produzcan errores en los intentos de cambiar la contraseña de NSX Appliance para los usuarios `root`, `admin` o `audit` en vSphere Client.

Causa

Durante la instalación de NSX Manager, el procedimiento solo acepta una contraseña para las tres funciones. Se podría producir un error al intentar cambiar esta contraseña más tarde.

Solución

- Utilice las API de NSX para cambiar las contraseñas.

  Para obtener más información, consulte https://kb.vmware.com/s/article/70691 y la *Guía de administración de NSX-T Data Center*.

Solucionar problemas de flujos de trabajo con errores e instancias de NSX Edge inestables

Si se produce un error en los flujos de trabajo o las instancias de NSX Edge son inestables, puede realizar los pasos de solución de problemas.

Problema

Al cambiar la configuración del grupode puertos distribuidos en vSphere Client, se pueden producir errores en los flujos de trabajo y las instancias de NSX Edge pueden volverse inestables.

Causa

Por diseño, no se permite la eliminación ni la modificación de los grupos de puertos distribuidos para la superposición y el vínculo superior que se crearon durante la fase de configuración del clúster de NSX Edge de los ajustes del clúster.

Solución

Si necesita cambiar la configuración de la VLAN o del grupo de direcciones IP de las instancias de NSX Edge, primero debe eliminar los elementos de NSX-T Data Center y la configuración de vSphere with Tanzu del clúster.

Para obtener información sobre cómo eliminar elementos de NSX-T Data Center, consulte la *Guía de instalación de NSX-T Data Center*.

Recopilar paquetes de soporte para la solución de problemas de NSX-T

Puede recopilar paquetes de soporte en los nodos de clúster y tejido registrados para solucionar problemas y descargar los paquetes en su máquina o cargarlos en un servidor de archivos.

Si decide descargar los paquetes en su máquina, obtendrá un solo archivo de almacenamiento compuesto por un archivo de manifiesto y paquetes de soporte para cada nodo. Si elige cargar los paquetes en un servidor de archivos, el archivo de manifiesto y los paquetes individuales se cargan en el servidor de archivos por separado

Procedimiento

1 Desde el navegador, inicie sesión con privilegios de administrador en un NSX Manager.

2 Seleccione **Sistema > Paquete de soporte**.

3 Seleccione los nodos de destino.

   Los tipos de nodos disponibles son **Nodos de administración** , **Edge**, **hosts** y **Puertas de enlace de nube pública**.

4 (opcional) Especifique la antigüedad del registro en días para excluir los registros que sean más antiguos que la cantidad especificada de días.

5 (opcional) Alterne el conmutador que indica si se deben incluir o excluir los registros de auditoría y los archivos principales.

   Nota Estos pueden contener información confidencial, como contraseñas o claves de cifrado.

6 (opcional) Active la casilla de verificación para cargar los paquetes a un servidor de archivos.

7 Haga clic en **Iniciar la recopilación de paquetes** para iniciar la recopilación de paquetes de soporte.

   La cantidad de archivos de registro de cada nodo determina el tiempo que se tarda en recopilar paquetes de soporte.

8 Supervise el estado del proceso de recopilación.

   La pestaña **Estado** muestra el progreso de la recopilación de paquetes de soporte.

9 Haga clic en **Descargar** para descargar el paquete si la opción para enviarlo a un servidor de archivos no se ha establecido

Recopilar archivos de registro de NSX-T

Puede recopilar los registros que se encuentran en los componentes de vSphere with Tanzu y NSX-T Data Center para detectar errores y solucionarlos. Los archivos de registro pueden solicitarse a través del soporte de VMware.

Procedimiento

1 Inicie sesión en vCenter Server mediante vSphere Client.

2 Recopile los siguientes archivos de registro.

Archivo de registro	Descripción
`/var/log/vmware/wcp/wcpsvc.log`	Contiene información relacionada con la habilitación de vSphere with Tanzu.
`/var/log/vmware/wcp/nsxd.log`	Contiene información relacionada con la configuración de los componentes de NSX-T Data Center.

3 Inicie sesión en NSX Manager.

4 Recopile el archivo `/var/log/proton/nsxapi.log` para obtener información sobre el error que NSX Manager devuelve cuando se produce un error en una operación de vSphere with Tanzu específica.

Reiniciar el servicio WCP si cambian la dirección IP, la huella digital o el certificado de administración de NSX-T

Si la dirección IP, la huella digital o el certificado de administración de NSX-T cambian después de instalar vSphere with Tanzu, debe reiniciar el servicio `WCP`.

Reiniciar el servicio vSphere with Tanzu si cambia el certificado de NSX-T

En este momento, si la dirección IP, la huella digital o el certificado de NSX-T cambian, vSphere with Tanzu requiere que el servicio `WCP` se reinicie para que el cambio surta efecto. Si el cambio ocurre sin reiniciar el servicio, se produce un error en la comunicación entre vSphere with Tanzu y NSX-T, y pueden surgir ciertos síntomas, como que NCP ingrese en la etapa CrashLoopBackoff o que los recursos del clúster supervisor no se puedan implementar.

Para reiniciar el servicio `WCP`, utilice `vmon-cli`.

1 Ejecute SSH en vCenter Server e inicie sesión como usuario raíz.

2 Ejecute el comando `shell`.

3 Ejecute el comando `vmon-cli -h` para ver las opciones y la sintaxis de uso.

4 Ejecute el comando `vmon-cli -l` para ver el proceso de `wcp`.

Verá el servicio `wcp` en la parte inferior de la lista.

5 Ejecute el comando `vmon-cli --restart wcp` para reiniciar el servicio `wcp`.

Verá el mensaje `Completed Restart service request`.

6 Ejecute el comando `vmon-cli -s wcp` y compruebe que se haya iniciado el servicio `wcp`.

Por ejemplo:

```
root@localhost [ ~ ]# vmon-cli -s wcp
Name: wcp
Starttype: AUTOMATIC
RunState: STARTED
RunAsUser: root
CurrentRunStateDuration(ms): 22158
HealthState: HEALTHY
FailStop: N/A
MainProcessId: 34372
```

VDS requerido para el tráfico del nodo de transporte del host

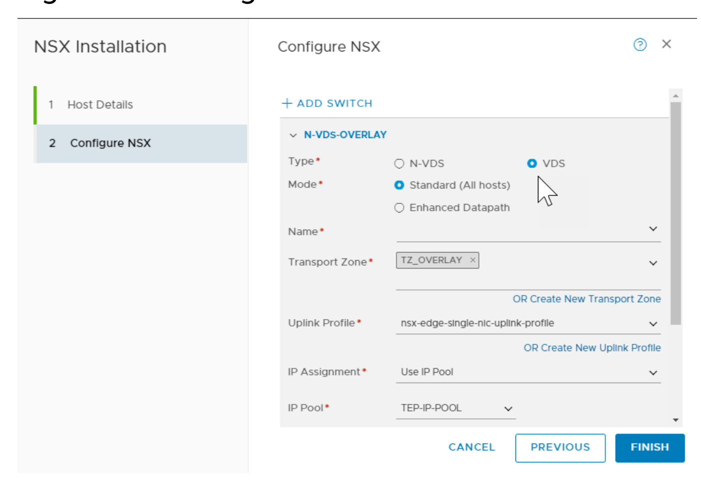
vSphere with Tanzu requiere el uso de un conmutador virtual distribuido (Virtual Distributed Switch, VDS) de vSphere 7 para el tráfico del nodo de transporte del host. No puede utilizar el VDS de NSX-T (N-VDS) para el tráfico del nodo de transporte del host con vSphere with Tanzu.

Se requiere VDS

vSphere with Tanzu requiere un VDS convergente que admita el tráfico de vSphere 7 y de NSX-T 3 en el mismo VDS. En las versiones anteriores de vSphere y NSX-T, cuenta con un VDS (o VSS) para el tráfico de vSphere y un N-VDS para el tráfico de NSX-T. Esta configuración no es compatible en vSphere with Tanzu. Si intenta habilitar la administración de cargas de trabajo usando un N-VDS, el sistema informa que el clúster de vCenter no es compatible. Para obtener más información, consulte Solucionar errores de compatibilidad del clúster para habilitar la administración de cargas de trabajo.

Para utilizar un VDS convergente, cree un VDS de vSphere 7 mediante vCenter y, en NSX-T, especifique este VDS al preparar los hosts ESXi como nodos de transporte. No alcanza con disponer de VDS-DSwitch en el lado de vCenter. VDS-DSwitch 7.0 debe configurarse con un perfil de nodo de transporte de NSX-T, tal como se describe en el tema Crear un perfil de nodo de transporte a continuación.

Figura 19-1. Configuración de VDS en NSX-T



Si actualizó a vSphere 7 y NSX-T 3 desde versiones anteriores, debe desinstalar el N-VDS de cada nodo de transporte de ESXi y volver a configurar cada host con una instancia de VDS. Póngase en contacto con VMware Global Support Service para obtener instrucciones.

Solucionar problemas de NSX Advanced Load Balancer

Puede solucionar los problemas de NSX Advanced Load Balancer que puede encontrar durante la actualización.

Recopilar paquetes de soporte para la solución de problemas

Para solucionar problemas de NSX Advanced Load Balancer, puede recopilar paquetes de soporte. Es posible que el Soporte técnico de VMware solicite los paquetes de soporte.

Cuando genere el paquete de soporte, obtendrá un único archivo descargable para los registros de depuración.

Procedimiento

1 En el panel de control Controlador AVI, haga clic en el menú situado en la esquina superior izquierda y seleccione **Administración**.

2 En la sección **Administración**, seleccione **Sistema**.

3 En la pantalla **Sistema**, seleccione **Soporte técnico**.

4 Para generar un paquete de diagnósticos, haga clic en **Generar soporte técnico**.

5 En la ventana **Generar soporte técnico**, seleccione **Registros de depuración** y haga clic en **Generar**.

6 Una vez generado el paquete, haga clic en el icono de descarga para descargarlo en su máquina.

Solucionar problemas de actualización de la topología de red

Cuando instala la versión 7.0 Update 1c de vSphere with Tanzu o actualiza el clúster supervisor desde la versión 7.0 Update 1 a la versión 7.0 Update 1c, la topología de red se actualiza desde una topología de puerta de enlace de nivel 1 única a una topología que tiene una puerta de enlace de nivel 1 para cada espacio de nombres dentro del clúster supervisor.

Puede solucionar los problemas que puede encontrar durante la actualización.

Error en la comprobación previa de la actualización debido a que no hay suficiente capacidad en el equilibrador de carga de Edge

Se produce un error en la comprobación previa de la actualización y el mensaje de error indica que no el equilibrador de carga no tiene suficiente capacidad.

Problema

El proceso de comprobación previa a la actualización genera un error con un mensaje que indica que la capacidad del equilibrador de carga es menor que la capacidad que necesita el clúster supervisor.

Solución

Realice uno de los siguientes pasos para solucionar el problema:

- Para forzar la actualización, haga clic en el botón **Forzar actualización** en el mensaje de error o utilice la línea de comandos vCenter Server con la marca `--ingnore-precheck-warnings true`.

  Nota Esta solución se recomienda solo si el clúster de Edge puede admitir las cargas de trabajo de espacios de nombres existentes. De lo contrario, se podrían omitir estas cargas de trabajo durante la actualización.

- Elimine las cargas de trabajo no utilizadas.
- Agregue otros nodos de Edge al clúster.

Se omitieron espacios de nombres de cargas de trabajo del clúster supervisor durante la actualización

Durante la actualización del clúster supervisor no se actualizaron algunas cargas de trabajo del espacio de nombres.

Problema

La actualización del clúster supervisor se realiza correctamente pero se omiten algunas cargas de trabajo del espacio de nombres durante la actualización. Los recursos de Kubernetes indican que los recursos son insuficientes y el estado de la puerta de enlace de nivel 1 que se acaba de crear es `ERROR`.

Causa

La capacidad del equilibrador de carga no es suficiente para admitir las cargas de trabajo.

Solución

Realice uno de los siguientes pasos para solucionar el problema:

- Elimine las cargas de trabajo que no se utilicen, reinicie NCP y vuelva a ejecutar la actualización.
- Agregue nodos de Edge adicionales al clúster y active una reasignación a la puerta de enlace de nivel 1. Reinicie NCP y vuelva a ejecutar la actualización.

Servicio de equilibrador de carga omitido durante la actualización

Durante la actualización del clúster supervisor, algunos servicios del equilibrador de carga no se actualizan.

Problema

La actualización del clúster supervisor se realiza correctamente, pero se omiten algunos servicios del equilibrador de carga de Kubernetes durante la actualización.

Causa

La cantidad de servicios de tipo de equilibrador de carga de Kubernetes en las cargas de trabajo del clúster supervisor y el clúster de Tanzu Kubernetes asociado supera el límite de servidores virtuales de NSX Edge.

Solución

Elimine las cargas de trabajo que no se utilicen, reinicie NCP y vuelva a ejecutar la actualización.

Solucionar problemas de clústeres de Tanzu Kubernetes

Para solucionar los problemas de los clústeres de Tanzu Kubernetes, tiene que conectarse a cualquier nodo del clúster, visualizar la jerarquía de recursos del clúster y recopilar los archivos de registro.

Recopilar paquete de soporte para clústeres de Tanzu Kubernetes

Para solucionar los errores de clústeres de Tanzu Kubernetes, puede ejecutar una utilidad que permita recopilar un paquete de registros de diagnóstico.

VMware proporciona la utilidad TKC Support Bundler que se puede utilizar para recopilar archivos de registro de clústeres de Tanzu Kubernetes y solucionar problemas.

Para obtener y usar la utilidad, consulte el artículo Cómo recopilar un paquete de registros de diagnóstico de un clúster de Tanzu Kubernetes (80949) en la base de conocimientos de soporte de VMware.

Solucionar errores de conexión de vCenter Single Sign-On

Si no tiene suficientes permisos en el espacio de nombres de vSphere, no puede conectarse a clúster supervisor o a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.

Problema

El complemento de vSphere para kubectl devuelve el mensaje de error `Error from server (Forbidden)` cuando intenta conectarse a una instancia de clúster supervisor o a un clúster de Tanzu Kubernetes como usuario de vCenter Single Sign-On.

Causa

No tiene permisos suficientes en el espacio de nombres de vSphere o no tiene acceso al clúster.

Solución

Si es un ingeniero de desarrollo y operaciones que trabaja con el clúster, compruebe con el administrador de vSphere que se le hayan concedido los permisos **Editar** de espacio de nombres de vSphere. Consulte Creación y configuración de un espacio de nombres de vSphere.

Si es un desarrollador que utiliza el clúster para implementar cargas de trabajo, compruebe con el administrador de clústeres que se le haya concedido el acceso al clúster. Consulte Conceder acceso de desarrollador a clústeres de Tanzu Kubernetes.

Solucionar errores de la biblioteca de contenido suscrita

Si la biblioteca de contenido suscrita alcanza los límites de la capacidad de almacenamiento, no podrá aprovisionar los clústeres de Tanzu Kubernetes.

Problema

Cuando se intenta aprovisionar un clúster de Tanzu Kubernetes, no se pueden extraer elementos de la biblioteca de contenido suscrita y aparece el siguiente error:

```
Internal error occurred: get library items failed for.
```

Causa

La biblioteca de contenido suscrita alcanzó su capacidad máxima. La biblioteca de contenido está respaldada por el almacenamiento conectado. Con el paso del tiempo, a medida que se publican más versiones de Kubernetes y se introducen archivos OVA en la biblioteca, el almacenamiento podría llenarse hasta completar su capacidad.

Solución

Migre a una nueva biblioteca de contenido. Consulte Migrar clústeres de Tanzu Kubernetes a una nueva biblioteca de contenido.

Solucionar errores de la biblioteca de contenido local

Consulte este tema para solucionar errores comunes de la biblioteca de contenido local.

No se puede encontrar TKR en clúster supervisor

Las bibliotecas de contenido locales se pueden utilizar en entornos restringidos de Internet. Para crear una biblioteca de contenido local, consulte Crear, proteger y sincronizar una biblioteca de contenido local para versiones de Tanzu Kubernetes.

Al aplicar la directiva de seguridad a la biblioteca de contenido, versión de Tanzu Kubernetes (TKR) en clúster supervisor no se mostrará si existe una de las siguientes condiciones.

- El paquete OVF de la biblioteca de contenido no está firmado.
- El paquete OVF está firmado con un certificado no válido.
- El paquete OVF está firmado con un certificado que no es de confianza para la instancia de vCenter Server donde está configurada la biblioteca de contenido local.

Solucionar errores de aprovisionamiento de clústeres

Si ha aprovisionado un clúster de Tanzu Kubernetes, pero las máquinas virtuales del plano de control no se inician, es posible que deba cambiar el tamaño o la clase de las máquinas virtuales.

Problema

Ha aprovisionado un clúster de Tanzu Kubernetes. El sistema está intentando encender las máquinas virtuales del plano de control, pero se produce un error con el siguiente mensaje:

```
The host does not have sufficient CPU resources to satisfy the reservation.
```

Causa

El tamaño o la clase de la máquina virtual no son suficientes para la implementación del clúster.

Solución

Cambie el tipo o la clase de la máquina virtual. Consulte Clases de máquina virtual para clústeres de Tanzu Kubernetes.

Solucionar errores de implementación de cargas de trabajo

Es posible que se produzcan errores de implementación de carga de trabajo si PodSecurityPolicy y los enlaces no están configurados para los usuarios autenticados.

Problema

La carga de trabajo de un contenedor se implementa en un clúster de Tanzu Kubernetes, pero la carga de trabajo no se inicia. Aparece un error similar al siguiente:

```
Error: container has runAsNonRoot and image will run as root.
```

Causa

Los clústeres de Tanzu Kubernetes se aprovisionan con la controladora de admisión de PodSecurityPolicy habilitada. Ningún usuario autenticado puede crear pods con privilegios o sin privilegios hasta que el administrador de clústeres enlace PodSecurityPolicy a los usuarios autenticados.

Solución

Cree un enlace adecuado al PodSecurityPolicy predeterminado o defina una versión personalizada de PodSecurityPolicy. Consulte Usar las directivas de seguridad de pods con clústeres de Tanzu Kubernetes y Tutorial del libro de visitas de Tanzu Kubernetes.

Solucionar errores de clase de máquina virtual

Las clases de máquinas virtuales deben estar enlazadas al espacio de nombres de vSphere para clústeres de Tanzu Kubernetes y clases de máquina virtual.

Error de enlace de clase de máquina virtual

Las clases de máquinas virtuales deben estar enlazadas al espacio de nombres de vSphere. Consulte Asociar una clase de máquina virtual con un espacio de nombres en vSphere with Tanzu. Si no asocia la clase de máquina virtual con el espacio de nombres, recibirá un error de `VirtualMachineClassBindingNotFound` similar al siguiente:

```
conditions:
  - lastTransitionTime: "2021-04-25T02:50:58Z"
    message: 1 of 2 completed
    reason: VirtualMachineClassBindingNotFound @ Machine/test-cluster
    severity: Error
    status: "False"
    type: ControlPlaneReady
  - lastTransitionTime: "2021-04-25T02:49:21Z"
    message: 0/1 Control Plane Node(s) healthy. 0/2 Worker Node(s) healthy
    reason: WaitingForNodesHealthy
    severity: Info
    status: "False"
    type: NodesHealthy
```

Reiniciar un trabajo de actualización con errores del clúster de Tanzu Kubernetes

Si se produce un error en la actualización de un clúster de Tanzu Kubernetes, puede reiniciar el trabajo de actualización y volver a intentar la actualización.

Problema

La actualización de un clúster de Tanzu Kubernetes falla y, como consecuencia, el estado del clúster es `upgradefailed`.

Causa

Se pueden producir errores en la actualización de un clúster por diferentes motivos, uno de los cuales es un almacenamiento insuficiente. Para reiniciar un trabajo de actualización con errores y volver a intentar la actualización del clúster, complete el siguiente procedimiento.

Solución

1 Inicie sesión en clúster supervisor como administrador. Consulte Conectarse al clúster supervisor como usuario vCenter Single Sign-On.

2 Busque `update_job_name`.

```
kubectl get jobs -n vmware-system-tkg -l "run.tanzu.vmware.com/cluster-namespace=$
{cluster_namespace},cluster.x-k8s.io/cluster-name=${cluster_name}"
```

3 Ejecute `kubectl proxy` de modo que `curl` se pueda utilizar para enviar solicitudes.

```
kubectl proxy &
```

Debería ver `Starting to serve on 127.0.0.1:8001`.

Nota No puede utilizar `kubectl` para revisar o actualizar el `.status` de un recurso.

4 Con `curl`, emita el siguiente comando de revisión para aumentar el valor de `.spec.backoffLimit`.

```
curl -H "Accept: application/json" -H "Content-Type: application/json-patch+json"
--request PATCH --data '[{"op": "replace", "path": "/spec/backoffLimit", "value": 8}]'
http://127.0.0.1:8001/apis/batch/v1/namespaces/vmware-system-tkg/jobs/${update_job_name}
```

5 Con `curl`, emita el siguiente comando de revisión para borrar `.status.conditions` de modo que la controladora de trabajo cree nuevos pods.

```
$ curl -H "Accept: application/json" -H "Content-Type: application/json-patch+json"
--request PATCH --data '[{"op": "remove", "path": "/status/conditions"}]'
http://127.0.0.1:8001/apis/batch/v1/namespaces/vmware-system-tkg/jobs/${update_job_name}/
status
```

Solución de problemas de administración de cargas de trabajo

Consulte esta sección para solucionar problemas relacionados con la administración de cargas de trabajo o si necesita recopilar un paquete de soporte para .

Recopilar el paquete de soporte para la administración de cargas de trabajo

Siga este procedimiento para recopilar el paquete de soporte para la administración de cargas de trabajo.

Complete la siguiente tarea para extraer los registros de clúster supervisor. Esto se puede hacer incluso si el clúster está bloqueado en estado de error o configurándose.

Procedimiento

1 Inicie sesión en su entorno de vSphere with Tanzu mediante vSphere Client.

2 Seleccione **Menú > Administración de cargas de trabajo**.

3 Seleccione la pestaña **Clústeres**.

4 Seleccione el clúster supervisor de destino.

5 Seleccione **Exportar registros**.

Resultados

Una vez que haya recopilado el paquete de soporte, consulte el siguiente artículo de la base de conocimientos: Cómo cargar información de diagnóstico para VMware a través del portal de FTP seguro: http://kb.vmware.com/kb/2069559.

Poner en cola el archivo de registro de administración de cargas de trabajo

Poner en cola el archivo de registro de administración de cargas de trabajo puede ayudar a solucionar problemas de habilitación y errores de implementación del clúster supervisor.

Solución

1 Establezca una conexión SSH con vCenter Server Appliance.

2 Inicie sesión como usuario `root`.

3 Ejecute el comando `shell`.

   Verá lo siguiente:

```
Shell access is granted to root
root@localhost [ ~ ]#
```

4 Ejecute el comando siguiente para poner el registro en cola.

```
tail -f /var/log/vmware/wcp/wcpsvc.log
```

Solucionar errores de compatibilidad del clúster para habilitar la administración de cargas de trabajo

Siga estos consejos para la solución de problemas si el sistema indica que el clúster de vSphere no es compatible con la habilitación de la administración de cargas de trabajo.

Problema

La página **Administración de cargas de trabajo** indica que el clúster de vCenter es incompatible cuando se intenta habilitar la administración de cargas de trabajo.

Causa

Esto puede deberse a varios motivos. En primer lugar, asegúrese de que el entorno cumpla con los requisitos mínimos para habilitar la administración de cargas de trabajo:

- Licencia válida: VMware vSphere 7 Enterprise Plus con el complemento para Kubernetes
- Al menos dos hosts ESXi
- DRS totalmente automatizado
- vSphere HA
- vSphere Distributed Switch 7.0
- Suficiente capacidad de almacenamiento

Si el entorno cumple con estos requisitos previos, pero el clúster de vCenter de destino no es compatible, utilice la CLI del centro de datos (Datacenter CLI, DCLI) de VMware para identificar los problemas.

Solución

1. SSH a vCenter Server.
2. Inicie sesión como usuario raíz.
3. Ejecute el comando `dcli` para mostrar la ayuda de la CLI del centro de datos de VMware.
4. Enumere los clústeres de vCenter disponibles ejecutando el siguiente comando de DCLI.

   ```
   dcli com vmware vcenter cluster list
   ```

   Por ejemplo:

   ```
   dcli +username VI-ADMIN-USER-NAME +password VI-ADMIN-PASSWORD com vmware vcenter cluster
   list
   ```

   Resultado de ejemplo:

   ```
   |-----------|---------|------------|----------|
   |drs_enabled|cluster  |name        |ha_enabled|
   |-----------|---------|------------|----------|
   |True       |domain-d7|vSAN Cluster|True      |
   |-----------|---------|------------|----------|
   ```

5 Compruebe la compatibilidad del clúster de vCenter ejecutando el siguiente comando de DCLI.

```
dcli com vmware vcenter namespacemanagement clustercompatibility list
```

Por ejemplo:

```
dcli +username VI-ADMIN-USER-NAME +password VI-ADMIN-PASSWORD com vmware vcenter
namespacemanagement clustercompatibility list
```

El siguiente resultado de ejemplo indica que, en el entorno, falta un conmutador VDS de NSX-T compatible.

```
|---------|----------|----------------------------------------------------------------------
-------------------|
|cluster  |compatible|
incompatibility_reasons                                                                |
|---------|----------|----------------------------------------------------------------------
-------------------|
|domain-d7|False     |Failed to list all distributed switches in vCenter 2b1c1fa5-
e9d4-45d7-824c-fa4176da96b8.|
|         |          |Cluster domain-d7 is missing compatible NSX-T
VDS.                                       |
|---------|----------|----------------------------------------------------------------------
-------------------|
```

6 Ejecute más comandos de DCLI según sea necesario para determinar otros problemas de compatibilidad. Además de errores de NSX-T, otros motivos comunes de incompatibilidad son los problemas de conectividad de DNS y NTP.

7 Para solucionar el problema, siga los pasos que se indican a continuación.

   a Ponga en cola el archivo `wcpsvc.log`. Consulte Poner en cola el archivo de registro de administración de cargas de trabajo.

   b Desplácese hasta la página **Administración de cargas de trabajo** y haga clic en **Habilitar**.

Apagar e iniciar el dominio de carga de trabajo de vSphere with Tanzu

Para evitar la pérdida de datos y mantener operativos los componentes y las cargas de trabajo del entorno de vSphere with Tanzu, debe seguir el orden especificado al apagar o iniciar los componentes.

Por lo general, las operaciones de inicio y apagado se realizan después de aplicar una revisión, actualizar o restaurar el entorno de vSphere with Tanzu.

La solución vSphere with Tanzu, incluidos los clústeres de Tanzu Kubernetes aprovisionados por servicio Tanzu Kubernetes Grid, forma parte del centro de datos definido por software (SDDC) de vSphere. Por lo tanto, debe tener en cuenta toda la pila de infraestructura de vSphere al apagar e iniciar el entorno de vSphere with Tanzu. Consulte el siguiente conjunto validado de procedimientos para el apagado y el inicio del SDDC de vSphere incluido vSphere with Tanzu:

- SDDC de vSphere incluido el procedimiento de apagado de vSphere with Tanzu
- SDDC de vSphere incluido el procedimiento de inicio de vSphere with Tanzu